Modélisation graphique probabiliste pour la maîtrise des risques, la fiabilité et la synthèse de lois de commande des systèmes complexes

Philippe Weber

UFR Sciences et Techniques Mathématiques Informatique Automatique
École Doctorale IAEM Lorraine

Habilitation à Diriger des Recherches

Université de Lorraine

par

Philippe WEBER

Modélisation graphique probabiliste pour la maîtrise des risques, la fiabilité et la synthèse de lois de commande des systèmes complexes

Soutenue publiquement le 8 juillet 2015

Composition du jury

Rapporteurs :

BERENGUER Christophe, Professeur à l'Institut national polytechnique de Grenoble
COCQUEMPOT Vincent, Professeur à l'Université Lille1 : Sciences et Technologies
LERAY Philippe, Professeur à L'Ecole Polytechnique de l'université de Nantes

Examinateurs :

PERES François, Professeur à l'Ecole Nationale d'Ingénieur de Tarbes (ENIT)
ZAMAI Eric, Maître de Conférences HDR à l'Institut national polytechnique de Grenoble
ZIO Enrico, Professeur l'Ecole Centrale Paris
IUNG Benoit, Professeur à l'Université de Lorraine
THEILLIOL Didier, Professeur à l'Université de Lorraine

Centre de Recherche en Automatique de Nancy
CRAN— UMR 7039 CNRS–UHP–INPL

Table des Matières

Remerciements

Il n'est pas facile de remercier de manière exhaustive l'ensemble des personnes qui ont participé et contribué aux travaux de recherche présentés dans ce document et m'ont aidé à acquérir la maturité nécessaire à l'obtention de cette Habilitation à Diriger les Recherches.

Je tiens à remercier les membres du jury pour avoir accepté d'évaluer mon travail et pour la finesse de leurs analyses, en premier lieu Christophe BERENGUER, Vincent COCQUEMPOT et Philippe LERAY, pour avoir accepté d'en être les rapporteurs ; puis François PERES, Eric ZAMAI et Enrico ZIO pour leur implication comme examinateurs. Je tiens à remercier très chaleureusement mes parrains scientifiques : Benoit IUNG et Didier THEILLIOL qui m'ont guidé et soutenu durant toutes ces années de travail en commun.

Je remercie tout particulièrement Christophe SIMON, mon complice scientifique et ami, pour toutes nos contributions communes. Je voudrais aussi remercier Eric LEVRAT avec qui j'ai partagé de nombreuses discussions de travail entre autres. Merci à Élise MARCANDELLA pour son optimisme revivifiant et ses éclaircissements sur le développement durable.

Je remercie mes partenaires industriels, Carole DUVAL (EDF), Paul MUNTEANU et Lionel JOUFFE (Bayesia) pour leur confiance et les différents projets en communs.

Merci aussi aux doctorants que j'ai eu le plaisir d'encadrer : Fateh GUENAB, Abdeljabbar BEN SALEM, Aurélie LEGER, Ahmed KHELASSI, Gabriela OLIVA-MEDINA, Geoffrey FALLET FIDRY, Antonello DE GALIZIA ; pour leurs travaux de thèse sur lesquels s'adosse l'ensemble de mes recherches.

Je remercie aussi les membres des équipes du CRAN dont je fais partie, et plus particulièrement mes coauteurs : Dominique SAUTER, Christophe AUBRUN, Jean-Christophe PONSART, Frédérique BICKING.

Merci aux collègues qui nous permettent d'avancer en résolvant nos problèmes de logistique, de déplacement et administratifs : Sabine HURAUX, Anne PIANT et Maryse FERRY.

Je ne saurais terminer ces remerciements sans adresser mes plus chaleureux remerciements à ma famille, en particulier à ma femme Carole, qui veille à préserver mon équilibre et sur qui je peux m'appuyer en toutes circonstances et à mes enfants Loïc et Manon qui remplissent de bonheur ma vie de famille.

Introduction

Depuis la fin du 20ème siècle la perception que nous avons des objets technologiques a évolué et est passée du système constitué de plusieurs composants techniques, à des systèmes complexes, mettant en interaction différentes composantes techniques, humaines et organisationnelles. L'occurrence dans les années 80 des premiers accidents industriels majeurs comme l'explosion de Flixborough (Department of Transport, 1975), l'accident de Three Miles Island (Kemeny, 1979) ou encore le nuage toxique de Seveso (Seveso, 1982) a fait ressortir le rôle que joue l'Homme et son organisation dans la défaillance des systèmes techniques. L'analyse de ces accidents nous a appris que les composantes ne sont pas indépendantes d'où la nécessité de les considérer de façon conjointe lors de l'appréciation des risques des systèmes industriels. Aujourd'hui les objets technologiques que nous exploitons sont pris dans leur environnement et sont alors définis comme des systèmes sociotechniques complexes. L'accroissement de la complication sur l'axe technique s'est fait conjointement à l'apparition de la complexité issue de l'interdépendance entre les axes : technique, humain, organisationnel et environnemental. Un système est un ensemble d'éléments en interaction dynamique organisés en fonction d'un objectif. Les systèmes industriels sont bien souvent fractionnés en plusieurs entités interconnectées. La complexité d'un système est relative au nombre plus ou moins élevé d'interactions et de dépendances entre ses entités.

Face aux contraintes réglementaires auxquelles les systèmes industriels sont actuellement soumis, un haut niveau de maîtrise de ces risques doit être constamment démontré et prouvé (DeRocquigny, 2012). Il est nécessaire de maîtriser des systèmes sociotechniques avec des visions à des niveaux de plus en plus globaux. Pour répondre à ces besoins, la sûreté de fonctionnement doit faire évoluer ses pratiques, ses démarches d'analyses et d'aides à la décision. Les méthodes de la sûreté de fonctionnement, initialement focalisées sur l'objet technique dans une optique d'évaluation de sûreté intrinsèque, doivent prendre en compte un environnement étendu autour de cet objet technique. Les composantes humaine, organisationnelle, environnementale, entrent par nécessité dans le champ d'investigation. Ainsi, les entreprises ont besoin de se munir de moyens d'évaluation et d'anticipation pour maîtriser ou optimiser les conséquences de leurs activités sur la sécurité des biens et des Hommes, sur la société (impacts économiques et sociaux) et sur l'environnement.

Pour être capable de maîtriser les objets industriels que nous exploitons, aussi bien en matière de conception, que d'exploitation et de maintenance, il est nécessaire d'en extraire des modèles afin d'en prévoir le fonctionnement ainsi que leurs évolutions. L'extraction d'un modèle est toujours conditionnée par un objectif. En sûreté de fonctionnement les objectifs peuvent être très variés, par exemple mes travaux de recherche se sont focalisés sur les objectifs suivants :

- Les modèles ont pour objectif d'évaluer l'impact des actions de maintenance sur le maintien en conditions opérationnelles du système et ainsi aider l'ingénieur dans la prise de décisions en maintenance.

- Les modèles ont pour objectif d'évaluer l'impact des actions de conduite et de commande sur la dégradation ou la détérioration en cas de dérive (défaut) ou de défaillance d'une partie du système et ainsi permettre de satisfaire les objectifs (la qualité des services délivrés) du système sans risque pour les utilisateurs, pour les opérateurs de conduite, pour l'environnement etc.

- Les modèles ont pour objectif d'évaluer l'efficacité des moyens mis en œuvre pour garantir un niveau de risque acceptable quelles que soient les contraintes opérationnelles et les perturbations environnementales et climatiques du système.

Les secteurs d'application de la sûreté de fonctionnement sont larges. Ils peuvent être liés à des vues très différentes : comme les modes de management, la gouvernance, le facteur humain, ils peuvent aussi être liés aux événements naturels (extrêmes) et à leurs conséquences sur la société, enfin ils peuvent être liés à la maintenance, la conduite et la réduction des risques de systèmes sociotechniques.

Malheureusement, la plupart des ingénieurs n'ont pas les moyens (outils, méthodes) pour interpréter de manière efficace les informations (connaissances et observations) relatives aux contraintes opérationnelles et aux perturbations qui conditionnent le fonctionnement de ces systèmes sociotechniques. Ceci constitue un véritable verrou pour la maîtrise des systèmes sociotechniques. Les phénomènes mis en cause sont complexes de par leur hétérogénéité et le nombre important d'imbrications de mécanismes de différentes natures qui les constituent. De plus, il n'existe pas de modèles analytiques précis permettant de décrire avec exactitude la totalité des phénomènes. Enfin, il est bien souvent impossible de connaître exactement l'état du système avant de prendre une décision, car l'état des composants n'est, en général, pas directement ou instantanément observable. Devant ce constat il est nécessaire que de nouvelles méthodes soient mises en œuvre pour résoudre ce problème.

Aujourd'hui, pour atteindre les objectifs désirés, il est nécessaire de modéliser les systèmes ainsi que leurs composants avec un nombre fini d'états ou de niveaux de fonctionnement : le système et les composants sont dits multi-états. En outre, le comportement des composants est conditionné par les contraintes opérationnelles et les perturbations environnementales du système. Dans ces cas, l'évaluation de la sûreté de fonctionnement devient difficile car elle doit prendre en compte les effets de combinaison des défaillances qui ne sont pas indépendantes de par les contraintes, les perturbations et par la nature multi-état des composants du système. Le résultat est un développement d'une grande quantité de scénarios à modéliser qui devient fastidieux pour l'analyste.

Cependant, des évaluations quantitatives sont indispensables pour garantir la viabilité et l'atteinte des objectifs des systèmes par rapport à des niveaux de risques et à leur sûreté de fonctionnement. Il est donc nécessaire de manipuler une représentation incertaine du système pour décrire son fonctionnement mais aussi ses dysfonctionnements. Cette

perception imparfaite est en faveur de l'utilisation d'une évaluation probabiliste de l'état du système. Les difficultés sont liées à l'intégration de grandes quantités d'informations pour modéliser ces systèmes industriels subissant de nombreuses interactions avec l'environnement. Pour répondre à ce problème de modélisation, j'ai choisi d'étudier la voie de la modélisation probabiliste. Les avancées de l'Intelligence Artificielle (IA), telles que les Réseaux Bayésiens (RB), apportent des formalismes efficaces de modélisation pour la prise de décisions de maintenance, de conduite ou de réduction des risques des systèmes industriels complexes. En 2004, le Massachusetts Institute of Technology (MIT) publie le classement des dix premières technologies appelées à révolutionner le monde industriel dans les années à venir : l'exploitation des réseaux bayésiens apparaît en 4ème position.

La contribution majeure de mes travaux est de formaliser des méthodes de modélisation graphique probabiliste telles que les RB pour résoudre différents problèmes liés à la sûreté de fonctionnement des systèmes complexes. Ma contribution est orientée vers l'application et le transfert de techniques de modélisation vers l'industrie. Je ne défends pas dans ce manuscrit une recherche algorithmique, mais la formalisation d'une méthodologie de construction de modèle basée sur la maîtrise des formalismes de modélisation pour répondre à des problèmes industriels. Mon travail est donc fortement lié à mes contacts avec des industriels de divers secteurs d'activités : EDF, SOREDAB, INERIS, CHU-Nancy, RATP, Dassault Aviation, Renault, SNCF. Ma situation d'enseignant responsable de la formation en maintenance et en sûreté de fonctionnement en école d'ingénieur (ESSTIN) contribue à conserver un contact important avec le milieu industriel (Sonovision, Assetsman, SPIE, Dalkia) et me permet un transfert des connaissances vers les ingénieurs. Enfin, une relation privilégiée avec la société BAYESIA me permet de travailler avec un éditeur de logiciel pour la recherche et le développement. BAYESIA a une partie de son activité en sûreté de fonctionnement et maîtrise des risques industriels et commercialise ses progiciels au niveau international.

Ma démarche a pour objet de faire le lien entre des formalismes mathématiques de modélisation et leurs utilisations par des industriels. Cette démarche est intéressante car elle demande de mettre en relation d'une part des concepts mathématiques pointus et d'autre part les problèmes industriels à résoudre en sûreté de fonctionnent. Cette démarche permet de remonter les besoins des industriels ; et mon travail en collaboration avec des chercheurs en informatique permet le développement des fonctionnalités supplémentaires dans les plateformes logicielles de modélisation. Il me semble important dans cette démarche de :

- généraliser et homogénéiser à partir de plusieurs problèmes industriels, des verrous scientifiques en les déclinant selon les enjeux (risque, fiabilité, commande et maintenance), mais en gardant de la cohérence et de l'applicabilité par rapport aux problèmes réels,
- formaliser et faire évoluer les méthodes pour répondre à des problèmes émergeant des industriels,
- faire en sorte que ces nouvelles démarches aillent au-delà du cercle restreint de leurs spécialistes pour devenir des méthodes reconnues pour l'analyse des systèmes, en promouvant ces méthodes et à terme en faisant évoluer les normes.

Dans cette démarche j'ai cherché à résoudre deux classes de problèmes :

- La modélisation en maîtrise des risques, en maintenance et en fiabilité pour des systèmes sociotechniques complexes ;
- L'intégration des connaissances de fiabilité dans la commande et le diagnostic des systèmes automatisés.

Les objectifs de mes travaux ont donc été de contribuer à :

- La modélisation de systèmes complexes pour l'aide à la décision dans un univers incertain : en proposant une méthode adaptées aux nouveaux enjeux de la sûreté de fonctionnement visant à évaluer des systèmes sociotechniques complexes.
- La prise en compte de la propagation des incertitudes dans la modélisation de systèmes complexes : en particulier l'incertitude sur l'évolution de l'environnement d'exploitation, l'incertitude sur la propagation des évènements dans l'évaluation probabiliste de sûreté, mais aussi dans le cas d'incertitude épistémique, c'est à dire le manque de connaissance.
- L'évaluation conjointe des risques multisectoriels : en intégrant les risques organisationnels et humains dans les analyses.
- La maîtrise du vieillissement des composants, l'anticipation des interventions de maintenance et de sécurité en fonction du vieillissement.
- La prolongation de durée d'exploitation : avec comme objectif d'assurer la sécurité, la maîtrise des risques et la qualité dans le cas d'une exploitation malgré la présence de dérives (défauts) ou de défaillances partielles d'un système.
- La pertinence des allocations de commande afin de réduire le risque en fonction de la criticité des composants et l'adaptation de la commande aux conditions d'exploitation et à l'état de santé des composants.

Pour résoudre ces problèmes, mes travaux de recherche se sont focalisés sur les formalismes de modélisation, et tout particulièrement les modèles graphiques probabilistes que sont les Réseaux Bayésiens (RB).

La modélisation par RB n'est pas encore totalement acceptée dans le milieu industriel car le formalisme mathématique RB ne possède pas intrinsèquement une sémantique liée à la sûreté de fonctionnement. De plus, ce formalisme de modélisation ne fait pas encore partie des méthodes de modélisation préconisés par les normes (NF EN 61 025 ; NF EN 61 078 ; NF EN 61 165 ; NF EN 62 502 ; NF EN 62 551). Les questions posées aujourd'hui par les ingénieurs sur la modélisation par RB portent principalement sur la validité des modèles et des estimations obtenues.

La preuve de la validité des algorithmes d'inférence ayant été faite (Pearl 1988), seule persiste la question de la validité du modèle construit par l'analyste. Les RB offrent un formalisme de modélisation général dans un univers incertain. Par conséquent, le défi aujourd'hui concernant la modélisation de la sûreté de fonctionnement par RB est de définir une méthodologie de modélisation qui n'est pas spécifique à un cas d'étude particulier mais une véritable méthodologie générique pouvant servir de référence.

Pour décrire mes activités de recherche ce rapport d'habilitation à diriger les recherches est organisé en quatre chapitres.

Le chapitre 1 présente mon Curriculum Vitae ; il est constitué de quatre sections décrivant : ma situation actuelle (établissement d'affectation, parcours professionnel et diplômes) ; une synthèse très concise de mes activités pédagogiques en enseignement ; et une synthèse de mes activités de recherche et d'encadrement (mes participations aux instances organisationnelles scientifiques, mon activité d'encadrement doctoral, le positionnement de mes activités de recherche, mon rayonnement scientifique et mes activités de coopération industrielle et de valorisation). La dernière section est consacrée à un bilan de ma production scientifique avec une analyse de mes co-auteurs et une liste classée de mes publications.

Le chapitre 2 permet de décrire mes activités d'enseignement et d'administration. Après une première section d'introduction, la section deux présente mes responsabilités pédagogiques et administratives. Le profil de mes enseignements en lien avec mes activités de recherche fait l'objet de la section trois. Les sections quatre et cinq présentent mes activités d'encadrement de stages et de projets et les enseignements faits en dehors de mon établissement. Enfin la dernière section présente une conclusion mettant en avant les relations entre mes activités d'enseignement, mes activités de recherche et les orientations de mon projet d'enseignement.

Le chapitre 3, qui est le plus conséquent, présente mes activités de recherche. Après une introduction de ma problématique de recherche, les quatre sections suivantes présentent les principaux résultats auxquels j'ai apporté ma contribution en faisant le lien entre mes collaborations industrielles et les différentes thèses que j'ai encadrées.

- Ainsi la section deux présente les réseaux bayésiens comme un formalisme de modélisation pour la sûreté de fonctionnement. Dans cette section nous faisons le lien entre distribution de probabilité jointe et description de fiabilité de système.
- La section trois présente les réseaux bayésiens comme un formalisme élégant et facile de mise en œuvre pour la modélisation de la fonction de structure des systèmes complexes et multi-états. Nous présentons les applications industrielles qui illustrent l'efficacité de ce formalisme de modélisation dans des cas réels.
- La section quatre concerne la modélisation par réseaux bayésiens dynamiques comme formalisme de représentation de la fiabilité des composants d'un système intégrant l'impact de l'environnement et des conditions d'exploitation. Cette section présente les différents modèles de composants puis l'agrégation de plusieurs processus stochastiques au sein d'un modèle multi-état dynamique du système.
- Enfin la section cinq décrit les premiers résultats sur l'intégration de la fiabilité à la commande des systèmes continus basés sur la modélisation par réseaux bayésiens dynamiques. Nous présentons une revue des travaux faisant le lien entre fiabilité et commande en positionnant nos travaux de recherche. Puis une proposition de structuration de la commande intégrant un réseau bayésien dynamique est proposée. Enfin les résultats de simulation d'une application à un système de distribution d'eau potable sont commentés, mettant en perspective les avantages de cette méthode.

La dernière section de ce chapitre présente une conclusion intégrant une liste de mes contributions en dégageant les trois apports majeurs à la communauté scientifique de mon travail de recherche.

Le chapitre 4 décrit mon projet de recherche. La première section explique les trois axes de recherche que je souhaite développer à court, moyen et long terme. Ces axes sont : l'intégration de connaissances probabilistes dans la stratégie de commande des systèmes dynamiques ; la modélisation probabiliste en maîtrise des risques des systèmes sociotechniques et leurs impacts sur le développement durable ; et enfin la formalisation de modèles graphiques probabilistes en sûreté de fonctionnement pour de nouvelles classes de systèmes. La section deux décrit les collaborations support de mon projet de recherche selon les trois axes, elle fait aussi état des projets et thèses qui devraient en découler. La section trois présente mon projet de rayonnement scientifique, avec la définition des actions d'animation scientifique locales, nationales et internationales. Une conclusion synthétique sur le déroulement de mes travaux de recherche sur ces 20 dernières années et leurs continuités vient clore ce chapitre.

Chapitre 1

Curriculum Vitae

1 Situation actuelle

Philippe WEBER, né le 13/02/1971 à Thionville (57), marié, deux enfants.

Grade : Maître de Conférences, classe normale, 6ème échelon, 61ème section du CNU, nommé en septembre 2000 et titularisé en septembre 2001 ;

Titulaire d'une **PEDR** (2009 – 2012) puis d'une **PES** niveau A (2013-2016).

1.1 Etablissement d'affectation

Enseignant à : Ecole Supérieure des Sciences et Technologies de l'Ingénieur de Nancy (ESSTIN), Université de Lorraine.
2 Rue Jean Lamour, 54509 Vandoeuvre-lès-Nancy, Cedex France
Téléphone : +33 383 685 127 Portable : +33 607 251 732 Fax : +33 383 685 001
Web : http://www.esstin.uhp-nancy.fr ; e-mail : Philippe.weber@univ-lorraine.fr

Chercheur au : Centre de Recherche en Automatique de Nancy (CRAN), UMR 7039, Université de Lorraine - CNRS.
Faculté des Sciences et Techniques - B.P. 70239
54506 Vandoeuvre-lès-Nancy, Cedex France
Téléphone : +33 383 684 465 Portable : +33 607 251 732 Fax : +33 383 684 462
Web : http://www.cran.uhp-nancy.fr ; e-mail : Philippe.weber@univ-lorraine.fr

Profil : emploi n°: 61MCF0775, Maintenance industrielle et sûreté de fonctionnement des systèmes de production à l'Ecole Supérieure des Sciences et Technologies de l'Ingénieur de Nancy (ESSTIN), Université de Lorraine.

Thème de recherche : Maîtrise des Risques, Sûreté de fonctionnement, Maintenance, Diagnostic et Systèmes Tolérants aux Fautes.

1.2 Parcours professionnel

depuis 2000	**Maître de Conférences**, 61ème section CNU, CRAN, ESSTIN, Université de Lorraine.
1999-2000	**A.T.E.R.** 61ème section CNU, CRAN, ESSTIN, Nancy Université.
1996-1999	**Allocataire de recherche**, LAG, UMR 5528 CNRS INPG (ENSIEG) associée à l'UJF.

1.3 Diplômes

1996-1999	**Doctorat** : Automatique et Productique. *Institut National Polytechnique de Grenoble.* Soutenance 29 octobre 1999. **Sujet** : Estimation paramétrique appliquée au diagnostic des procédés. **Jury**: M. Luc DUGARD, Directeur de Recherche au CNRS, LAG, Président M. Dominique SAUTER, Professeur à l'UHP, CRAN, Nancy, Rapporteur M. Jean-Claude TRIGEASSOU, Professeur au LAII-ESIP, Poitiers, Rapporteur M. Jean Philippe CASSAR, Professeur à l'IAAL, Lille, Examinateur Mme. Sylviane GENTIL, Professeur à l'ENSIEG, Grenoble, Directeur de thèse
1995-1996	**Service national**, III° corps d'armée, 7° division blindée, 35 Régiment d'Infanterie, *Belfort.*
1994-1995	**DEA** : Automatique et Traitement Numérique du Signal, *option diagnostic* - mention assez bien. *Université Henri Poincaré, Nancy 1.* **Sujet :** Conception et Application d'un Outil de Diagnostic de Défauts Capteurs. **Rapport Bibliographique** : Système expert temps réel appliqué au diagnostic.
1993-1994	**Maîtrise** : Electronique Electrotechnique et Automatique (EEA), *option électronique* - mention assez bien. *Université Henri Poincaré, Nancy 1.*
1992-1993	**Licence** : Electronique Electrotechnique et Automatique (EEA). *Université Henri Poincaré, Nancy 1.*
1991-1992	**DEUG** : Science des Structures de la Matière, filière Sciences Physiques pour l'Ingénieur (SPI), *option électronique* - mention assez bien. *Université Henri Poincaré, Nancy 1.*
1989-1991	**DUT** : Génie Electrique et Informatique Industrielle (GEII), *option électronique* – mention assez bien. *Institut Universitaire de Technologie (IUT) de Longwy.*
1988-1989	**Baccalauréat** : série E Mathématiques, Physique et Technologie. *Lycée Technique Les Grand Bois 57000 Hayange*.

2 Synthèse des activités pédagogiques

2.1 Responsabilités administratives de formation

Membre du Groupe de Réflexions sur le Programme Pédagogique (GRPP) de l'ESSTIN de 2003 à 2007.

Responsable de l'option ESSTIN - Maintenance Industrielle (MI) de 2004 à 2005.

Responsable des relations industrielles, des projets et stages de l'option ESSTIN - Maintenance Industrielle (MI) de 2005 à 2008

Responsable pédagogique de l'option ESSTIN - Maintenance Industrielle (MI) de 2008 à 2010.

Responsable pédagogique de l'option ESSTIN - Maintenance et Sûreté des Systèmes (MSS) depuis 2011.

Responsable des contrats de professionnalisation de l'option ESSTIN - Maintenance et Sûreté des Systèmes (MSS) depuis 2012.

2.2 Enseignement des connaissances

Depuis 2000 : Cours à l'ESSTIN, et encadrement de projets et stages d'ingénieurs (niveau L et M).

Depuis 2009 : Cours de Master en Ingénierie des Systèmes Complexes (ISC) de l'UL, et encadrement de projets et stages master (niveau M).

Depuis 2003 : co-encadrement des doctorants de l'École Doctorale IAEM Lorraine (niveau D).

2.3 Enseignement des connaissances issues de la Recherche

Cours International niveau master 2 en anglais

Weber P., 20h de cours : "FAULT DIAGNOSIS (FDI) AND FAULT TOLERANT CONTROL (FTC) USING RELIABILITY ANALYSIS", Centro Nacional de Investigación (CENIDET) Interior Internado Palmira s/n, Col. Palmira. Cuernavaca, Morelos: Mexique, 9-14 June (2008).

Cours en France niveau master 2 dans d'autres établissements

Weber P., 4h de cours : Application des Réseaux Bayésiens à l'Analyse des performances de Processus. Enseignement de cours de 3ème année à l'Ecole Centrale Paris. Présenté de 2002 à 2003.

Weber P., 4h de cours : Réseaux Bayésiens pour l'Analyse de sûreté de fonctionnement. Enseignement de cours de 3ème année à l'ENSEM filière ISA, module 582, Mise en œuvre de la sûreté de fonctionnement ; Présenté de 2004 à 2009.

3 Synthèse des activités de recherche et d'encadrement

3.1 Participation aux instances organisationnelles scientifiques locales

Conseil du Laboratoire

Membre nommé du Conseil du Laboratoire CRAN (2006-2008)

Membre élu du Conseil du Laboratoire CRAN (2008-2012)

Membre nommé du bureau du Conseil du Laboratoire CRAN (2008-2012)

Membre élu du Conseil du Laboratoire CRAN (2013-2017)

Commission de Spécialistes et Comité de Sélection

Membre (suppléant) élu de la Commission de Spécialistes de l'UHP, Nancy 1 - 61ème section (2006 - 2008)

Membre (suppléant) élu de la Commission de Spécialistes de Nancy 2 -

31/60/61/62/63ème sections (2006 - 2008)

Membre nommé du Comité de Sélection pour le poste 61_MCF-0213 de l'UHP, Nancy 1 - 61ème section (2011)

Commission Information Scientifique et Technique

Membre de la commission Information Scientifique et Technique (IST) du CRAN (2013 - 2017).

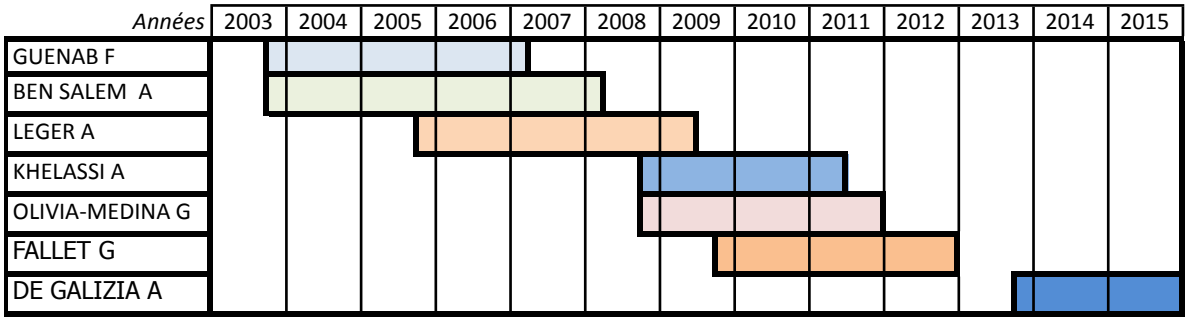
Animations Scientifiques au CRAN

Animation du groupe de réflexion : Chercheurs et enseignants-chercheurs à l'occasion de la visite AERES (2012).

3.2 Encadrement doctoral

Codirections de thèses (6)

Table 1 : Co-encadrement de thèses.



Comme l'illustre le Tableau 1, j'ai co-encadré les 6 doctorats suivants :

GUENAB F. (2007) : Contribution aux systèmes tolérants aux défauts : Synthèse d'une méthode de reconfiguration et/ou de restructuration intégrant la fiabilité des composants. Thèse de doctorat de Nancy Université, 20 février, (150 pages). Encadrement : Pr. D. THEILLIOL 50%, P. WEBER 50%, du 01/10/2003 au 20/02/2007.

Durée : 40 mois ; Financement : sur projet européen IFATIS, puis sur poste d'ATER. Situation du docteur : Ingénieur consultant en Informatique.
Publications : 1 revue, 6 conférences internationales, 1 conférence nationale.

BEN SALEM A. (2008) : Modèles Probabilistes de Séquences Temporelles et Fusion de Décisions. Application à la Classification de Défauts de Rails et à leur Maintenance. Thèse de doctorat de Nancy Université, 7 mars, (138 pages). Encadrement : Pr. B. IUNG 50%, P. WEBER 50%, du 01/10/2003 au 07/03/2008 en cotutelle avec l'INRETS : Laurent Bouillaut et Patric Aknin.

Durée : 42 + 12 mois (**interruption de la thèse durant 12 mois avant la soutenance**) ; Financement : 36 mois cofinancement INRETS – CRAN (Région Lorraine) ; 6 mois ATER ; 12 mois salarié ingénieur sûreté de fonctionnement chez Bombardier Transport France ; Situation du docteur : Manager, Bombardier Transport UK Ltd.
Publications : 4 conférences internationales, 1 conférence nationale.

LEGER A. (2009) : Contribution à la formalisation unifiée des connaissances fonctionnelles et organisationnelles d'un système industriel en vue d'une évaluation quantitative des risques et de l'impact des barrières envisagées. Thèse de doctorat de Nancy Université,

28 mai, (226 pages). Encadrement : Pr. B. IUNG 20%, P. WEBER 40%, E. LEVRAT 40%, du 17/10/2005 au 28/05/2009.

Durée : 44 mois ; Financement : CIFRE, EDF-CRAN, puis ATER ; Situation du docteur : Ingénieur - Chercheur EDF R&D France.
Publications : 2 revues, 4 conférences internationales, 1 conférence nationale.

KHELASSI A. (2011) : Nouvelle méthodologie de synthèse de lois de commande active tolérante aux fautes garantissant la fiabilité du système. Thèse de doctorat de Nancy Université, 11 juillet, (133 pages). Encadrement : Pr. D. THEILLIOL 50%, P. WEBER 50%, du 01/10/2008 au 11/07/2011.

Durée : 33 mois ; Financement : Bourse du MESR ; Situation du docteur : Ingénieur – Recherche ArcelorMittal Global R&D, France.
Publications : 2 revues, 10 conférences internationales, 1 conférence nationale.

OLIVA-MEDINA G. (2011) : Modélisation d'un système de production et de son environnement technique, humain et organisationnel par Réseaux Bayésiens Orientés Objet pour le choix de stratégies de maintenance. Thèse de doctorat de Nancy Université, 12 décembre, (198 pages). Encadrement : Pr. B. IUNG 50%, P. WEBER 50%, du 01/10/2008 au 12/12/2011.

Durée : 38 mois ; Financement : Allocation de recherche sur projet SKOOB, ANR PROJET 07 TLOG 021 ; Situation du docteur : en 2012 post doctorat CRAN, projet BMCI pôle MER Paca, depuis 2013 Ingénieur de recherche PREDICT.
Publications : 5 revues, 4 conférences internationales, 3 conférences nationales, 4 rapports.

FALLET G. (2012) : AiDR : Eléments pour l'amélioration de la robustesse et la propagation des incertitudes résiduelles. Thèse de doctorat de Nancy Université, 10 décembre, (225 pages). Encadrement : Pr. B. IUNG 50%, P. WEBER 50%, du 01/10/2009 au 10/12/2012.

Durée : 38 mois ; Financement : CIFRE, EDF-CRAN ; Situation du docteur : Ingénieur Projets ALCADIA.
Publications : 1 revue, 2 participations à ouvrage, 3 conférences internationales, 1 rapport.

Actuellement je codirige la thèse suivant :

DE GALIZIA A. : Evaluation probabiliste de l'efficacité de barrières humaines. Thèse de doctorat de l'Université de Lorraine en cours. Encadrement : Pr. B. IUNG 50%, P. WEBER 50%, du 15/10/2013 au 15/10/2016. Financement : CIFRE, EDF-CRAN.

Les publications avec les doctorants sont représentées de manière synthétique dans la Figure 1. La production scientifique moyenne des doctorants que j'ai encadrés est de : 1,8 revues internationales et 5,1 conférences internationales par doctorant.

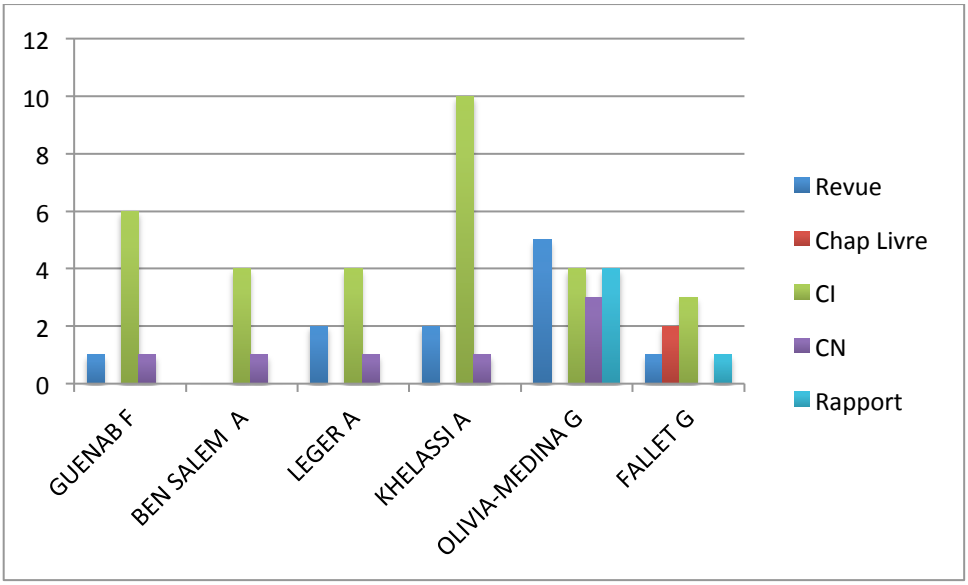


Figure 1 : Publications avec les doctorants encadrés

Encadrements de master (7)

J'ai encadré les 7 étudiants en stages de Master suivants :

KOUIDER M. (2000) **:** Prise en compte par la technique des **Réseaux Bayésiens** des contraintes liées à la Sûreté de Fonctionnement dans la phase de conception des systèmes automatisés. Stage de DEA-ATNS CRAN.

HORDAS P. (2001) **:** Outils d'une démarche TPM pour optimiser le lien entre la qualité du produit, la productivité et **l'efficacité de la maintenance**. Stage de DEA Production Automatisée (PA) CRAN. Situation actuelle : Manager chez PSA Peugeot Citroën.

FRANCOIS-RADA M. : Modélisation de la fiabilité d'équipements électromécaniques par les **réseaux bayésiens**. Stage de DEA Production Automatisée (PA) CRAN (2000-2001).

FALLET G. (2009) : **Estimation des risques** environnementaux, techniques, humains et organisationnels intégrés et propagation de données incertaines. Université Nancy 1 Henri Poincaré, Faculté des Sciences et Techniques, Master Recherche IS-EEAPR - Option P&R. Poursuite en thèse CIFRE CRAN-EDF.

MEYER K. (2010) : Fiabilisation d'une cellule d'usinage - MESSIER BUGATTI. Université Nancy 1 Henri Poincaré, Faculté des Sciences et Techniques, Master Ingénieries des Systèmes Complexes ISC – Option Sûreté et Sécurité Actives des Systèmes S3A. Situation actuelle : Ingénieur Spécialiste Fiabilité des Systèmes FAURECIA.

KARZAZI I. (2010) : Etude de complémentarité entre applications PLM et GMAO appliquées au secteur du maintien en conditions opérationnelles application chez LASCOM. Master Ingénieries des Systèmes Complexes ISC – Option Management Intégré de la Production de Biens et Services MIPBS. Situation actuelle : Consultant PLM- DASSAULT SYSTEMES.

HACHLAF A. (2011) : Contribution aux **systèmes tolérants aux défauts** : Synthèse d'une méthode active de réallocation dynamique des actionneurs intégrant un **modèle probabiliste dynamique de fiabilité**. Master Ingénieries des Systèmes Complexes ISC – Option Sûreté et Sécurité Actives des Systèmes S3A. Situation actuelle : en recherche d'emploi.

Synthèse quantitative

Codirections de thèse	7 (dont 1 en cours)
Encadrement de master	7

3.3 Positionnement de mes activités de recherche

Positionnement dans le laboratoire CRAN

Mes travaux de recherche sont menés au sein du Centre de Recherche en Automatique de Nancy (CRAN). Ils s'intègrent naturellement dans le département Ingénierie des Systèmes Eco-Techniques (ISET) sous la responsabilité des professeurs Benoît Iung et de André Thomas et dans le département Contrôle - Identification - Diagnostic (CID) sous la responsabilité des professeurs Didier Maquin et de Gilles Millerioux.

Dans le département ISET les recherches traitent des systèmes dans leurs environnements et en interaction avec leurs systèmes de soutien, c'est-à-dire les systèmes permettant le fonctionnement du système dit « principal ». Dans le département CID les recherches portent sur le contrôle, l'identification et le diagnostic de systèmes combinant des dispositifs interconnectés de nature différente. Les systèmes considérés sont complexes et mes activités de recherche, menées dans ces deux départements, ont pour objet de disposer d'une représentation globale et unifiée des systèmes ainsi que d'outils d'analyses des exigences de sûreté de fonctionnement ou de performances opérationnelles. Cette appartenance à deux départements résulte de mon profil de recherche, elle est totalement justifiée par une activité de recherche à la frontière entre les thématiques de ces deux départements. Ce positionnement est riche par la complémentarité des vues prises en compte et contribue aussi à mon approche originale.

Mes activités de recherche se placent plus précisément dans le projet : « Sûreté de Fonctionnement Système » (SdFS - ISET) dont le responsable est le professeur Jean François Pétin, et le projet : « Co-conception de systèmes dynamiques sûrs de fonctionnement » (CSDF-CID) dont le responsable est le professeur Didier Theilliol.

Le projet SdFS - ISET rassemble des recherches sur le développement des activités de Health Monitoring & Management pour évaluer des situations potentiellement dégradées des systèmes. Les recherches ont pour objectif d'analyser, pour les systèmes éco-techniques complexes, la sûreté de fonctionnement sous un angle « système » considérant de façon intégrée les paramètres de fiabilité, maintenabilité, disponibilité et sécurité (paramètres FMDS). Cette orientation soulève plusieurs verrous scientifiques notamment la modélisation stochastique et déterministe pour l'évaluation des paramètres de FMDS conjointe du système principal et de son système de soutien. Il est de plus nécessaire, du fait de la modélisation de systèmes éco-techniques complexes, de prendre en compte les problèmes de gestion de l'incertitude dans les modèles qu'elle soit structurelle ou paramétrique. Enfin, face à la problématique de construction des modèles dans le cas de grands systèmes et en lien avec leur complexité, la formalisation de modèles repose sur des méthodologies en utilisant le principe de définition de patrons (motif) pour aider à la structuration, la réutilisation, la maintenabilité d'un modèle global tout en assurant sa qualité (réduction de complexité, robustesse des résultats par rapport à la plage d'utilisation).

Le projet CSDF-CID concerne le développement de méthodes de synthèse de systèmes

reconfigurables intégrant, de façon coordonnée, la qualité de contrôle et la sûreté de fonctionnement dans une approche de co-conception. Il s'agit ainsi de développer des méthodes d'analyse et d'optimisation des propriétés structurelles des systèmes en intégrant, la fiabilité des composants pour le choix de la redondance matérielle ou analytique. L'objectif est de permettre, lors de la conception, d'évaluer et d'optimiser les propriétés de "diagnosticabilité", de "commandabilité", d'observabilité et de tolérance aux défauts en lien avec la fiabilité des composants. En exploitation, et c'est bien là l'un de mes axes de recherche, il s'agit de développer des méthodes de diagnostic de défauts et de commande tolérante aux défauts qui prennent en compte des indicateurs relatifs à la sûreté de fonctionnement formalisés notamment au travers de modèles probabilistes. Ces modèles permettent d'appréhender, de façon quantitative, le vieillissement des composants en relation avec les contraintes qu'ils subissent (environnement d'exploitation et de commande).

Positionnement académique

Mes travaux se positionnent d'un point de vue académique dans des thématiques nationales telles que :

- Les activités couvertes par le GIS - 3SGS : Surveillance, sûreté et sécurité des grands systèmes.
- Les thématiques développées dans les Groupes de Travail (GT) du Groupe de Recherche en Modélisation, Analyse, Conduite des Systèmes dynamiques (GdR MACS) ; Axe 2 (Modélisation, aide à la décision et supervision) : S3 (Sûreté / Surveillance / Supervision), SED (Systèmes à Événements Discrets) et MACOD (Modélisation et optimisation de la maintenance coopérative et distribuée).
- Mon travail trouve aussi place dans les manifestations et les projets scientifiques organisés par l'Institut pour la Maîtrise des Risques et la Sûreté de Fonctionnement (IMdR) et tout particulièrement dans le Groupe de Travail et de Réflexion : Réseaux probabilistes appliqués à la maîtrise des risques et à la sûreté de fonctionnement dont je suis l'animateur.
- Enfin au niveau de la région, mes travaux se retrouvent dans le CPER Lorraine. Mes recherches sont à classer dans le Pôle de recherche scientifique et technologique (PRST) en Modélisation, informations et système numérique (MISN) - projet : Sûreté et sécurité des systèmes (SSS).

D'un point de vue international mes activités de recherche sont en relation avec les thématiques soutenues par les instances suivantes :

- IFAC : La fédération internationale d'automatique qui a pour objectif de promouvoir la science et la technologie de contrôle dans le sens le plus large et pour tous les systèmes. Mes travaux sont en relation avec les thématiques abordées par les Technical Committees suivants : TC 3.1. Computers for Control ; TC 5.1. Manufacturing Plant Control ; TC 5.2. Manufacturing Modelling for Management and Control ; TC 6.3. Power and Energy Systems ; TC 6.4. Fault Detection, Supervision & Safety of Technical Processes-SAFEPROCESS.
- IEEE : Institute of Electrical and Electronics Engineers en particulier le IEEE Reliability Society qui a pour rôle de promouvoir les méthodes pour évaluer et assurer la sécurité et la fiabilité des systèmes dans un sens large et tout au long de du cycle de vie. Ses domaines d'intérêts englobent la conception, l'analyse, la production et l'évaluation des systèmes : informatique, réseaux, matériels... Le comité technique se

focalise sur la sécurité des réseaux, la disponibilité, maintenabilité, diagnostic, pronostic et la gestion de la santé, de la qualité, de la soutenabilité, l'ingénierie humaine, … et la sécurité du système.

- ESRA/ESREDA : L'association European Safety, Reliability and Data est une association européenne favorisant les échanges d'informations entre chercheurs et ingénieurs en matière de sécurité, de fiabilité et de sûreté des systèmes.
- UAI : L'Association pour l'incertitude en intelligence artificielle est axée sur l'organisation de la conférence annuelle sur l'incertitude en intelligence artificielle (UAI) et, plus généralement, sur la promotion de la recherche dans la poursuite des progrès dans la représentation des connaissances, l'apprentissage et le raisonnement dans l'incertain.

Contacts et/ou collaborations

D'un point de vue international, je suis en contact avec des chercheurs sur les axes de recherches suivants :

- Sur le plan de la modélisation de la fiabilité dans le problème de diagnostic et de commande tolérante aux défauts :
  - Université de Concordia, Pr. Youming Zhang, Canada.
  - Université de Barcelone, Pr. Vince Puig, Espagne.
- Sur le plan de la modélisation probabiliste appliquée à la sûreté de fonctionnement et plus particulièrement la modélisation par Réseaux Bayésiens :
  - Università del Piemonte Orientale, Pr. Luigi Portinale, Italie.
  - Queen Mary, University of London, Pr. Martin Neil, Angleterre.

3.4 Rayonnement scientifique international

Articles reconnus par les éditeurs de revues internationales (4)

Revue RESS : Top 10 Cited papers (articles published in the last five years 2005-2011)
Extracted from Scopus (on *Mon Feb 28 21:40:35 GMT 2011*).
Google Scholar Citations : >175

Weber P., Jouffe L., Complex system reliability modelling with Dynamic Object Oriented Bayesian Networks (DOOBN). Special Section - Selected Papers Presented at QUALITA 2003, guest editors J.F. Aubry in Reliability Engineering and System Safety, **91,** 2, (2006), 149-162.

Revue EAAI : Top Hottest articles, Engineering Applications of Artificial Intelligence.
N°3: Top Hottest articles in 2012 full year
N°4: The most cited articles published in the 5 years : 2010 to 2015, extracted from Scopus.
Google Scholar Citations : >125 en 3 ans

Weber P., Medina-Oliva G., Simon C., Iung B., Overview on Bayesian networks Applications for Dependability, Risk Analysis and Maintenance areas. Engineering Applications of Artificial Intelligence, **25**, 4, June (2012), 671-682, DOI:10.1016/j.engappai.2010.06.002

Revue JRR : Paper highly commended by the Editor and Editorial Board of the Journal of Risk and Reliability to : The Professional Engineering Publishing of Best Paper Award for papers published in the Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability in 2009.

The top five most cited articles in the 5 years : 2009 to 2014.

Simon C., Weber P., Imprecise reliability by evidential networks. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* **223**, 2, (2009), 119-131. DOI : 10.1243/1748006XJRR190

Léger A., Weber P., Levrat E., Duval C., Farret R., Iung B., Methodological developments for probabilistic risk analyses of socio-technical systems. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* **223**, 4, (2009), 313-332. DOI : 10.1243/1748006XJRR230

Organisation de sessions invitées (4)

J'ai organisé les sessions invitées suivantes :

Session invitée *Réseaux Bayésiens théorie et application à la sûreté de fonctionnement et à la qualité.* 5ème Congrès international pluridisciplinaire, Qualité et Sûreté de Fonctionnement, Qualita'03, Nancy, 18 mars, (2003).
Session chair: Weber Philippe, (CRAN), Université de Lorraine, CNRS UMR 7039.

Special session *on Bayesian Networks / Evidential Networks / Markov decision Process with Application in dependability and maintenance decision.* 16th Mediterranean Conference on Control and Automation, Ajaccio, Corsica, France (2008). (Technical Co-Sponsor: IEEE Control Systems Society).
Session co-chairs: Weber Philippe, (CRAN), Université de Lorraine, CNRS UMR 7039.
Wuillemin Pierre-Henri, (LIP6), Université Pierre & Marie Curie, CNRS UMR 7606.

Special session *on Bayesian Networks in Dependability.* IFAC Workshop on Dependable Control of Discrete System, DCDS'09, Bari : Italie (2009).
Session co-chairs: Montani Stefania, University of Piemonte Orientale, Italie.
Weber Philippe, Université de Lorraine, CNRS UMR 7039.

Special session *on Applications of Probabilistic Graphical Models in Dependability, Diagnosis and Prognosis.* IFAC 9th Safeprocess 2015, Symposium on Fault Detection, Supervision and Safety for Technical Processes, Paris : France (2014).
Session co-chairs: Weber Philippe, Université de Lorraine, CNRS UMR 7039.
Portinal Luigi, Computer Science Institute, DiSIT, University of Piemonte Orientale, Italie.

Sessions plénières internationales (2)

Theilliol D., Weber P., Khelassi A., Design of fault-tolerant control and fault diagnosis methods based on reliability. 10th International Conference in Diagnostics of Processes and Systems DPS, Zamość : Poland, September 19-21 (2011).

Weber P., Theilliol D., Networks Application to the Dependability of Multi-State Systems. 12th International Conference on Diagnostics of processes and systems, Ustka: Poland, September 7-9 (2015). (http://www.konsulting.gda.pl/dps2015/web/).

Séminaire international (1)

Weber P. Bayesian networks applications in dependability. Cenidet seminary, Cuernavaca, Morelos: Mexico, 10 June (2008).

Evaluation d'articles scientifiques

Je suis relecteur pour les revues internationales suivantes (18) :

Revues	*Facteur d'impact*
Information Sciences	
International Journal of Electrical Power and Energy Systems	
IEEE Trans. Reliability	Fi > 2
IEEE Trans. Systems, Man, and Cybernetics: Systems	
Reliability Engineering & Systems Safety	
International Journal of Approximate Reasoning	
IEEE Trans. Automation Science and Engineering	
Journal of Process Control	
Applied Mathematical Modelling	
IEEE Sensors Journal	Fi > 1
Safety Science	
Engineering Applications of Artificial Intelligence	
ISA Transaction	
Journal of Intelligent Manufacturing	
Annals of Operations Research journal	
Journal Theory and Decision	
Theory and Decision	Fi < 1
Journal of Risk and Reliability, Proceedings of the Institution of Mechanical Engineers Part O	

J'ai été relecteur pour de nombreuses conférences internationales :

IFAC : Safeprocess, Ifac World Congres, DCDS ; IEEE : MED ; IFIP : ARES ; Autres Label : ESREL, IAR, ACD, ...

Ainsi que pour World Scientific Publishing (1 livre).

Membre d'un groupe de travail scientifique international

Je suis membre en temps qu'expert en modélisation par réseaux bayésiens du groupe d'intérêt : « Technology and Process of Care in Emergency Care » faisant partie du « Research Committee of the European Society for Emergency Medicine (EuSEM)». La mission de ce groupe d'intérêt est la promotion de la recherche sur la modélisation probabiliste appliquée à la Médecine d'urgence.

Ce groupe d'intérêt, qui compte 12 membres, est animée par le Dr. Nathalie Flacke du Centre Hospitalier Charles Haby de Guebwiller et membre de l'« European Society for Emergency Medicine ». Nous avons communiqué les objectifs de ce groupe de travail lors de la conférence : German Society Interdisciplinary Emergency and Acute Medicine, 9th Annual Meeting DGINA (Flacke et al. 2014).

Synthèse quantitative Internationale

Articles reconnus (Awards)	4
Organisation de sessions invitées	4
Sessions plénières internationales	2
Séminaire international	1
Evaluation d'articles scientifiques	
en revues internationales	>20
en conférences	>10

3.5 Rayonnement scientifique national

Participation à des jurys de thèse en tant qu'examinateur (3)

Université d'Angers (2007)
Sylvain VERRON, Diagnostic et surveillance des processus complexes par réseaux bayésiens. Thèse dirigée par Pr. A. KOBI, préparée au sein du Laboratoire LASQUO dans l'école doctorale d'Angers, Institut des Sciences et Techniques de l'Ingénieur d'Angers, soutenue le 13 décembre 2007.

Université de Grenoble (2012)
Mohammed Farouk BOUAZIZ, Contribution à la modélisation Bayésienne de l'état de santé d'un système complexe : application à l'industrie du semi-conducteur. Thèse dirigée par E. Zamaï, préparée au sein du Laboratoire G-SCOP dans l'école doctorale EEATS, Université de Grenoble, soutenue le 27 novembre 2012.

Université de Paris Est (2014)
Rony ROZAS, Intégration du retour d'expérience pour une stratégie de maintenance dynamique. Thèse dirigée par Dr P. Aknin et Cr. L. Bouillaut, préparée au sein de l'IFSTTAR – Grettia, Université de Paris EST, soutenue le 19 décembre 2014.

Organisation de journées ou de conférences

J'ai participé à l'organisation de la deuxième session des Journées d'Actualisation en Maintenance Industrielle Intégrée (JAMII), thème : Management de la Maintenance, Longwy, 17 et 18 novembre, (1999).

J'ai fait partie du comité d'organisation du 5° Congrès international pluridisciplinaire Qualité et Sûreté de Fonctionnement, Qualita'03, Nancy, 18 mars, (2003).

J'ai co-organisé avec C. Simon, la journée IMdR-SdF & RUFEREQ sur le thème : « Réseaux Bayésiens : Méthodes et applications à la sûreté de fonctionnement et à la maîtrise des risques », Paris (France), 20 septembre, (2012).

Je fais partie du comité d'organisation du 11° Congrès international pluridisciplinaire Qualité et Sûreté de Fonctionnement, Qualita'15, Nancy, (2015).

J'ai fait partie des comités scientifiques de Qualita 2007…2015, Lambda Mu 2014.

Présentations invitées Nationales (9)

IMdR-SdF

Weber P., Modélisation de la fiabilité d'un système de chauffage complexe (Intérêt des réseaux bayésiens relativement aux méthodes de SdF). Journée IMdR-SdF, retour d'expérience : les réseaux bayésiens, outils d'analyse et de structuration. Paris (France), 29 Septembre (2005).

Simon C., **Weber P.,** Aubry JF., Des sous-ensembles flous aux fonctions de croyance: quelques applications pour les systèmes instrumentés de sécurité. Journée de l'IMdR-SdF sur les nouvelles théories de l'incertain, Paris (France), 17 Septembre (2008).

Weber P., Simon C., Introduction aux Réseaux Bayésiens et modélisation de la fiabilité. Journée IMdR-SdF & RUFEREQ sur le thème : « Réseaux Bayésiens : Méthodes et applications à la sûreté de fonctionnement et à la maîtrise des risques », Paris (France), 20 septembre (2012).

Simon C., **Weber P.,** Bicking F., Session Didactique : Quelques applications en fiabilité. Journée IMdR- SdF & RUFEREQ sur le thème : « Réseaux Bayésiens : Méthodes et applications à la sûreté de fonctionnement et à la maîtrise des risques », Paris (France), 20 septembre (2012).

Weber P., Simon C., Theilliol D., Puig V., Fault-Tolerant Control Design for over-actuated System conditioned by Reliability: a Drinking Water Network Application. IMdR-SdF & RUFEREQ Groupe de Travail et de Réflexion (GTR) : Réseaux probabilistes appliqués à la Maîtrise des Risques et à la Sûreté de Fonctionnement, Paris (France), 13 février (2013).

GDR MACS

Weber P., Application de la modélisation par Réseaux Bayésiens à la sûreté de fonctionnement. Séminaire S3 GDR MACS, 31 janvier (2008).

Weber P., Simon C., Theilliol D., Aubrun C., Bayesian networks to Reliability modeling: applications to fault Diagnosis and Reconfiguration. Journée du GT *ARC-GDR MACS*, ConecsSdF, Paris (France), 27-Jan (2011).

Pôle de Compétitivité HYDREOS

Weber P., C. Simon, D. Theilliol. Application des réseaux bayésiens à la problématique du contrôle des réseaux de distribution d'eau potable. Séminaire TIC et EAU, Solutions numériques pour la gestion de l'eau, Nancy : France, 24 novembre (2011).

ISA France

Weber P., Simon C., Theilliol D., Puig V., Aide à la décision pour la commande de système sur-actionné tolérant aux défaillances basé sur la fiabilité. Journée ISA France sur la Surveillance des procédés industriels : algorithmes de traitement et aides à la décision- Nancy, 17 octobre (2013).

Animation d'un groupe de travail scientifique national

Depuis 2013, je suis fondateur et animateur avec Christophe SIMON, d'un Groupe de Travail et de Réflexion (GTR) de l'Institut pour la Maîtrise des Risques (IMdR) : Réseaux probabilistes appliqués à la Maîtrise des Risques et à la Sûreté de Fonctionnement. Dans ce GTR qui

compte 30 participants, nous proposons de mettre en commun connaissances et compétences ; d'organiser des journées thématiques ; de mettre en évidence les points tant théoriques qu'applicatifs à développer ; d'élaborer une bibliothèque de référence ; de produire des documents de référence, ainsi que des guides sur l'exploitation des réseaux probabilistes en sûreté de fonctionnement.

Nous avons publié à l'issu de nos présentations dans ce groupe et sur invitation, trois articles dans la bibliothèque virtuelle de l'AFNOR. Ces articles ont pour objet de démontrer l'efficacité de la modélisation par réseau bayésien en sûreté de fonctionnement (Weber et Simon 2013, 2014 ; Duval et al. 2014). Cette activité me permet de conserver un contact avec des industriels et universitaires. Ces relations sont importantes car elles me permettent de faire émerger des projets de collaboration nationale.

Synthèse quantitative nationale

Participation à des jurys de thèse	3
Organisation de manifestations scientifiques	4
Présentations invitées nationales	9
Animation d'un groupe de travail national	1

3.6 Coopérations industrielles et valorisations

Application de mes travaux

En France mes travaux en lien avec la maîtrise des risques sont appliqués sur des systèmes de production d'énergie électrique, principalement dans le secteur nucléaire en lien avec le département de Maîtrise des Risques Industriels (MRI) de EDF.

Mes travaux sur la partie commande et reconfiguration des systèmes sont appliqués à la reconfiguration du convertisseur d'énergie dans les éoliennes en partenariat avec le LIEN et le GREEN de l'Université de Lorraine.

A l'international mes travaux sur la partie commande et reconfiguration des systèmes sont appliqués à la commande de réseaux de distribution d'eau potable en relation avec l'Université de Barcelone, à la commande de drone quadri-rotor en partenariat avec l'Université de Concordia.

Projets de recherches européens (3)

- European Community's FP6 : « Intelligent FAult Tolerant control in Integrated Systems » IFATIS (EU-IST-2001-32122-IFATS), (2002-2005), Collaboration de 19 partenaires (42 mois). J'interviens sous le label « CRAN – Centre de recherche en automatique de Nancy » en tant qu'expert sûreté de fonctionnement en relation avec les travaux de thèse de Fateh Guenab sur une méthode de reconfiguration et/ou de restructuration intégrant la fiabilité des composants.
- European Community's FP7 : « Dynamic Decisions in Maintenance » Dynamite (SP6-IST-NMP-2-017498), (2005 - 2009), Collaboration de 16 partenaires (42 mois). J'interviens sous le label « Université Henri Poincaré Nancy I » en tant qu'expert sûreté de

fonctionnement et Réseaux Bayésiens en relation avec les travaux de thèse d'Alexandre Muller sur le pronostic.

- European Community's FP7 : F3 Factory (2009 - 2013), work packages WP9 - Dissemination, Collaboration de 25 partenaires (48 mois). J'interviens sous le label « Institute National Polytechnique de Lorraine » en tant qu'expert sûreté de fonctionnement et Maintenance de l'UL.

Porteur de projets de recherches nationaux (2)

- Projet industriel EDF IDAFH (2004), (12 mois) :
  Collaboration CRAN/EDF (IDAFH)
  Financement total : 19 500 Euros - Financement perçu par le CRAN : 13 000 Euros.
- Projet ANR technologie logiciel SKOOB (2008-2011), (36 mois)
  Collaboration CRAN/LIP6/BAYESIA/EDF/SOREDAB/ERPI/CHU Nancy/INERIS (SKOOB)
  Financement total : 1,2M Euros - Financement perçu par le CRAN : 117 076 Euros.

Participation à des projets de recherches nationaux (9)

- Projet de prestation : UHP UNI (2001) prestation pour PSA Peugeot Citroën, (6 mois).
- Projet de prestation : UHP – APIP (2005), prestation pour DCN dans le cadre du GT MACODE du GDR MACS.
- Projet GIS 3SGS : COSMOS (Conception et Observation de Systèmes à Mode multiples de fonctionnements Sûrs – Design of Safety Systems based on Multi Working Modes) (2008-2009), Collaboration LAGIS/ICD/CReSTIC/CRAN (12 mois)
- Projet CPER Lorraine : Plate-fOrme ModulAire dédiée aux Energies EOLiennes – FTC for Wind Turbines (Pomadeol) (2008-2010), collaboration CRAN/GREEN/LIEN (24 mois)
- Projet GIS 3SGS : MARATHON (2009-2012), collaboration CRAN/EDF (36 mois)
- Projet IMdR-SdF : P04-7 Réseaux bayésiens et retour d'expérience en sûreté de fonctionnement (2010), collaboration Bayesia / CRAN (6 mois)
- Projet GIS 3SGS : SAFFE (Systèmes dynamiques tolérAnts aux Fautes et FiablEs – Ageing Management in Fault-tolerant control system design) (2010-2012), Collaboration CRAN/LAGIS/STMR (24 mois)
- Projet CPER Lorraine : Ecosur2 (Lot1) (2010-2014), collaboration CRAN/GREEN/LIEN (48 mois)
- Projet GIS 3SGS : SOMAIRE (2011-2012), collaboration LAMIH/EDF/CRAN (12 mois)

Porteur de conventions de thèses CIFRE (3)

Mes relations industrielles ont permis de signer 3 contrats de conventions de thèse CIFRE en liens avec mes travaux de recherche. Pour ces conventions j'ai été responsable scientifique (Leger, Fallet, De Galizia) et financier (Leger, De Galizia).

- CRAN-EDF-INERIS (CIFRE), Leger A. (2005-2008).
  Financement total : 279 046 Euros - Financement perçu par le CRAN : 41 856 Euros.
- CRAN-EDF (CIFRE), Fallet G. (2009-2012).
  Financement total : 215 000 Euros - Financement perçu par le CRAN : 30 000 Euros.
- CRAN-EDF (CIFRE), De Galizia A. (2013-2016).
  Financement total : 407 000 Euros - Financement perçu par le CRAN : 51 000 Euros.

Synthèse quantitative

Projets de recherches européens	3
Porteur de projets de recherches nationaux	2
Participation à des projets de recherche nationaux	9
Porteur de conventions de thèses CIFRE	3

4 Bilan de la production scientifique

4.1 Synthèse quantitative

Revues internationales indexées JCR	17
Revues internationales non indexées JCR	3
Revue nationale	1
Participation à la rédaction d'ouvrages	6
Rapports de thèse	1
Encadrement de thèse	6
Conférence internationale invitée	2
Conférences internationales en session invitée	5
Conférences internationales avec actes	50
Conférences nationales ou sans acte	25
Rapports et Notes internes du CRAN	14
Notes internes du LAG	3
Rapport de DEA	2

4.2 Analyse des co-auteurs principaux

La recherche ne se fait pas individuellement, les co-auteurs de mes publications se répartissent entre membres permanents du CRAN, chercheurs nationaux et internationaux, doctorants et industriels comme l'indique la Figure 2. Les pourcentages indiqués font référence aux 80 articles des catégories revues internationales et conférences internationales. Cette présentation permet de faire clairement apparaître les noms de mes principaux co-auteurs.

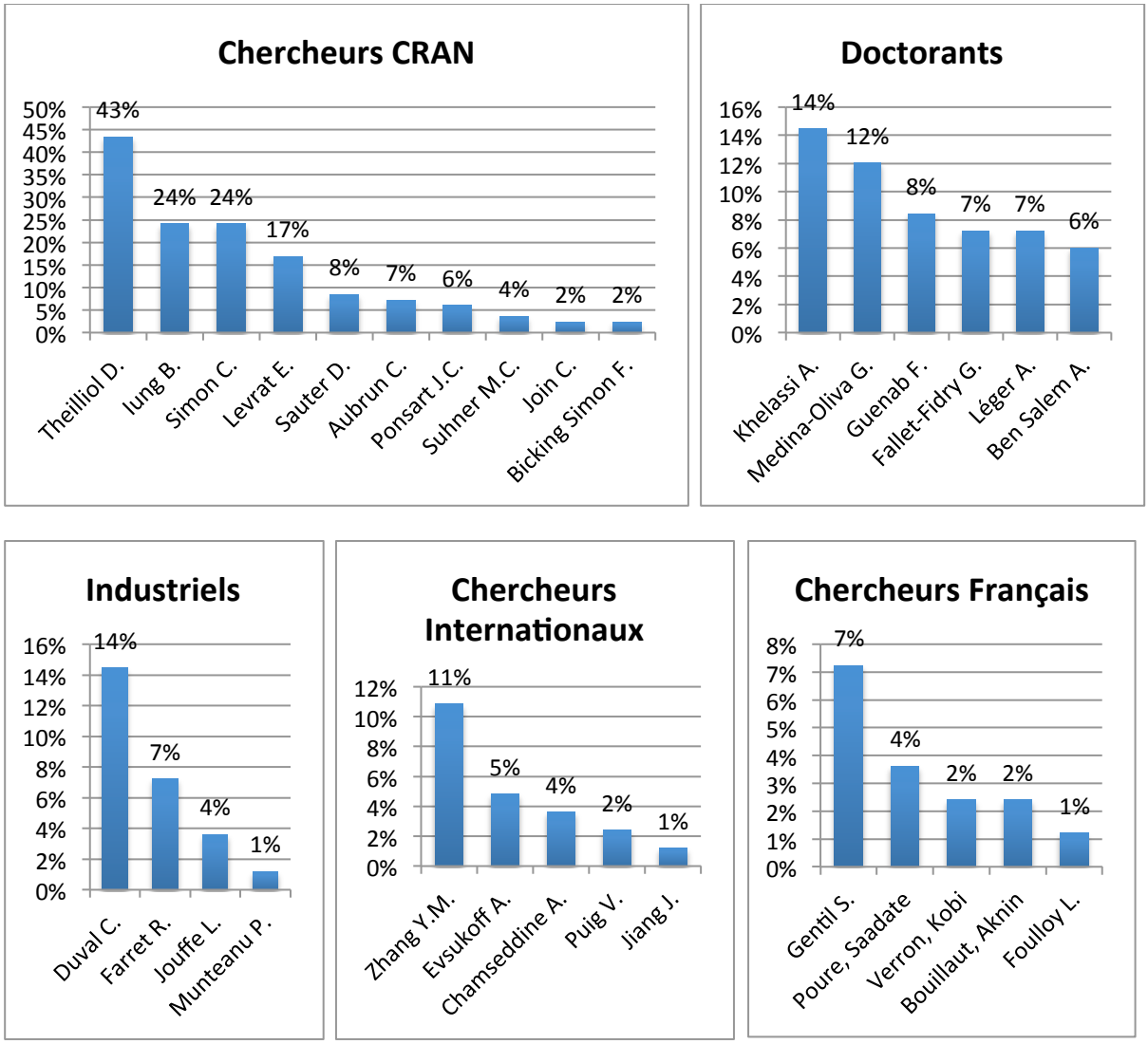


Figure 2 : Répartition des co-auteurs

4.3 Liste classée des publications [1]

Revues internationales (17)

Medina-Oliva G., **Weber P.**, Iung B. Industrial system knowledge formalization to aid decision making in maintenance strategie sassessment. *Engineering Applications of Artificial Intelligence*, **37**, (2015), pp. 343–360.

Chamseddine A., Theilliol D., Sadeghzadeh I., Zhang Y., **Weber P.** Optimal reliability design for over-actuated systems based on the MIT rule: Application to an octocopter helicopter testbed. *Reliability Engineering and System Safety*, **132**, (2014), pp. 196-206.

Medina-Oliva G., **Weber P.**, Iung B. PRM-based patterns for knowledge formalisation of industrial systems to support Maintenance Strategies Assessment. *Reliability Engineering and System Safety*, **116**, August (2013), pp. 38-56.

Duval C., Fallet-Fidry G., Iung B., **Weber P.,** Levrat E. A Bayesian network-based integrated risk analysis approach for industrial systems: application to heat sink system and

[1] Les auteurs soulignés (universitaires, industriels) sont externes au laboratoire ; les publications sont classées dans l'ordre anti-chronologique.

prospects development. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, **226**, 5, pp. 488–507, octobre (2012).

Weber P., Boussaid B., Khelassi A., Theilliol D., Aubrun C. Reconfigurable control design with integration of a reference governor and reliability indicators. *International Journal of Applied Mathematics and Computer Science (AMCS)*, **22**, 1, (2012a), pp. 139–148, DOI : 10.2478/v10006-012-0010-0

Weber P., Medina-Oliva G., Simon C., Iung B. Overview on Bayesian networks Applications for Dependability, Risk Analysis and Maintenance areas. *Engineering Applications of Artificial Intelligence*, **25**, 4, June (2012b), pp. 671-682, DOI:10.1016/j.engappai.2010.06.002

Iung B., Medina-Oliva G., **Weber P.,** Levrat E. Using probabilistic relational models for knowledge representation of production systems: A new approach to assessing maintenance strategies. *CIRP Annals - Manufacturing Technology*, **61**, 1, pp. 419–422, (2012).

Guenab F., **Weber P.,** Theilliol D., Zhang Y.M. Optimal Design of Fault Tolerant Control System versus Reliability Analysis under Dynamic Behaviour Constraints. *International Journal of Systems Science*, **42**, 1, (2011), pp. 219-233.

Khelassi A., Theilliol D., **Weber P**. Reconfigurability Analysis for Reliable Fault-Tolerant Control Design, *International Journal of Applied Mathematics and Computer Science* (AMCS), **21**, 3, (2011), pp. 431-439.

Poure P., **Weber P**., Theilliol D., Saadate S. Fault tolerant control of a three-phase three-wire shunt active filter system based on reliability analysis. Original Research Article, *Electric Power Systems Research*, **79**, 2, February (2009), pp. 325-334, DIO : 10.1016/j.epsr.2008.07.003 ; ISSN: 0378-7796

Simon C., **Weber P.** Evidential networks for reliability analysis and performance evaluation of systems with imprecise knowledge. *IEEE Transactions on Reliability*, **58**, 1, March (2009a), pp. 69-87. DOI : 10.1109/TR.2008.2011868

Simon C., **Weber P.** Imprecise reliability by evidential networks. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* **223**, 2, (2009b), pp. 119-131. DOI : 10.1243/1748006XJRR190

Léger A., **Weber P.,** Levrat E., Duval C., Farret R., Iung B. Methodological developments for probabilistic risk analyses of socio-technical systems. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* **223**, 4, (2009), pp. 313-332. DOI : 10.1243/1748006XJRR230

Weber P., Theilliol D., Aubrun C. Component Reliability in Fault Diagnosis Decision-Making based on Dynamic Bayesian Networks. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* **222**, 2, (2008), pp. 161-172. DOI : 10.1243/1748006XJRR96

Gama C.A., Evsukoff A.G., **Weber P.,** Ebecken N.F. Parameter Identification of Recurrent Fuzzy Systems with Fuzzy Finite-State Automata Representation. *IEEE Transactions on Fuzzy Systems*, **16,** 1, (2008), pp. 213-224.

Simon C., **Weber P.,** Evsukoff A.G. Bayesian networks inference algorithm to implement Dempster Shafer theory in reliability analysis. *Special Issue "Bayesian networks in dependability" guest editors Montani S. and Boudali H., in Reliability Engineering and System Safety,* **93**, 7, (2008), pp. 950-963. DOI : 10.1016/j.ress.2007.03.012

Weber P., Jouffe L. Complex system reliability modelling with Dynamic Object Oriented Bayesian Networks (DOOBN). Special Section - Selected Papers Presented at QUALITA

2003, guest editors J.F. Aubry, in *Reliability Engineering and System Safety*, **91,** 2, (2006), pp. 149-162.

Revues internationales non indexées JCR (3)

Medina-Oliva G., **Weber P.,** Levrat E., Iung B. Using object-oriented bayesian networks to model an industrial system: a new approach to assessing maintenance strategies. *Insight Journal of INCOSE,* **14**, 4, (2011), pp. 24-26. (Article court)

Léger A., Levrat E., **Weber P.,** Iung B., Duval C., Farret R. Methodology for a probabilistic risk analysis of socio-technical systems. *Insight Journal of INCOSE,* **11**, 3, (2008), pp. 25-26. (Article court)

Simon C., **Weber P.,** Levrat E. Bayesian Networks and Evidence Theory to Model Complex Systems Reliability, *Journal of Computers* (JCP), ISSN : 1796-203X, **2**, 1, February (2007), pp. 33-43.

Revue nationale (1)

Weber P., Suhner M. Modélisation de processus industriels par Réseaux Bayésiens Orientés Objet (RBOO) - Application à l'analyse des performances d'un processus industriel. *Revue d'intelligence artificielle*, **18,** 2, ISSN 0992-499X, avril (2004), pp. 299-326.

Participations à la rédaction d'ouvrages (6)

Duval C., Marle L., Paradowski V., Simon C., **Weber P.** Exemples d'application des réseaux Bayésiens. Dans BIVI Maîtrise des risques, (2014), pp. 1-21.

Bicking F., **Weber P.**, Theilliol D., Aubrun C. Control allocation using reliability measures for over-actuated systems. Dans Intelligent Systems in Technical and Medical Diagnostics (2014), pp. 487-497.

Weber P., Simon C. Réseaux bayésiens : un nouveau formalisme de modélisation pour la sûreté de fonctionnement. Dans BIVI Maîtrise des risques (2013), pp. 1-16.

Weber P., Simon C. Réseaux bayésiens : méthodologies de modélisation en sûreté de fonctionnement. Dans BIVI Maîtrise des risques (2013), pp. 1-29.

Fallet-Fidry G., Duval C., Simon C., Levrat E., **Weber P.,** Iung B. Maîtrise et analyse des risques des systèmes intégrant les domaines techniques, humains, organisationnels et environnementaux. Dans Jean Arlat, Nada Matta, Yves Vandenboomgaerde, éditeur : Supervision, surveillance et sûreté de fonctionnement des grands systèmes, Traité Information, Commande, Communication, IC2, 309–330. Hermès Science Publications, (2012a).

Fallet-Fidry G., Duval C., Simon C., Levrat E., **Weber P.,** Iung B. Risk analysis and management in systems integrating technical, human, organizational and environmental aspects. In Yves Vandenboomgaerde, Nada Matta et Jean Arlat, éditeurs : Supervision and Safety of Complex Systems, 368. Wiley-ISTE, août, (2012b). Chapter 14, ISBN 978-1-84821-413-2.

Rapport de thèse (1)

Weber P. Diagnostic de procéder par l'analyse des Estimations Paramétriques de Modèles de Représentation à temps Discret. Thèse de doctorat de l'Institut National Polytechnique de Grenoble, 29 octobre, (1999), (180 pages). (Disponible sur Internet : http://www-lag.ensieg.inpg.fr/publications/theses/1999.html)

Encadrements de thèse (6)

Guenab F. Contribution aux systèmes tolérants aux défauts : Synthèse d'une méthode de reconfiguration et/ou de restructuration intégrant la fiabilité des composants. Thèse de doctorat de Nancy Université, 20 février, (2007), (150 pages).

Ben Salem A. Modèles Probabilistes de Séquences Temporelles et Fusion de Décisions. Application à la Classification de Défauts de Rails et à leur Maintenance. Thèse de doctorat de Nancy Université, 7 mars, (2008), (138 pages).

Léger A. Contribution à la formalisation unifiée des connaissances fonctionnelles et organisationnelles d'un système industriel en vue d'une évaluation quantitative des risques et de l'impact des barrières envisagées. Thèse de doctorat de Nancy Université, 28 mai, (2009), (226 pages).

Khelassi A. Nouvelle méthodologie de synthèse de lois de commande active tolérante aux fautes garantissant la fiabilité du système. Thèse de doctorat de Nancy Université, 11 juillet, (2011), (133 pages).

Medina-Oliva G. Modélisation d'un système de production et de son environnement technique, humain et organisationnel par Réseaux Bayésiens Orientés Objet pour le choix de stratégies de maintenance. Thèse de doctorat de Nancy Université, 12 décembre, (2011), (198 pages).

Fallet G. AiDR : Eléments pour l'amélioration de la robustesse et la propagation des incertitudes résiduelles. Thèse de doctorat de Nancy Université, 10 décembre, (2012), (225 pages).

Conférence internationale Session plénière (2)

Theilliol D., **Weber P.,** Khelassi A. Design of fault-tolerant control and fault diagnosis methods based on reliability. 10th International Conference in Diagnostics of Processes and Systems DPS, Zamość : Poland, September 19-21 (2011).

Weber P., Theilliol D., Networks Application to the Dependability of Multi-State Systems. 12th International Conference on Diagnostics of processes and systems, Ustka: Poland, September 7-9 (2015). (http://www.konsulting.gda.pl/dps2015/web/).

Conférences internationales en session invitée (5)

Medina-Oliva G., **Weber P.,** Simon C., Iung B. Bayesian networks applications on dependability, risk analysis and maintenance. ***Session invitée,*** 2nd IFAC Workshop on Dependable Control of Discrete System, DCDS'09, Bari : Italie (2009a).

Weber P., Simon C. Dynamic evidential networks in system reliability analysis: A Dempster Shafer approach. ***Session invitée,*** 16th Mediterranean Conference on Control and Automation, Ajaccio, France, June 25-28, (2008), 603-608.

Simon C., **Weber P.** Bayesian Networks Implementation of the Dempster Shafer Theory to Model Reliability Uncertainty. ***Session invitée,*** Workshop on Bayesian Networks in Dependability (BND2006) in the First International Conference on Availiability, Reliability and Security, ARES 2006, Vienna, April 20-22, Autriche (2006), pp. 788-793.

Guenab F., Theilliol D., **Weber P.,** Zhang Y., Sauter D. Fault tolerant control system design: A reconfiguration strategy based on reliability analysis under dynamic behavior constraints. ***Session invitée***, 6th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, Beijing, P.R. China, (2006), pp. 1387-1392.

Guenab F., Join C., Ponsart J.C., Sauter D., Theilliol D., **Weber P.** A reliability approach to reconfiguration strategy: application to the IFATIS benchmark problem. ***Session***

invitee, 2nd IFAC Symposium on System Structure and Control. Oaxaca, Mexico, December 8-10, (2004a).

Conférences internationales avec actes (50)

Bicking F., Weber P., Aubrun C., Theilliol D. Control allocation using reliability measures for over-actuated system. Dans 11th International Conference on Diagnostics of Processes and Systems, DPS 2013 - 11th International Conference on Diagnostics of Processes and Systems, DPS 2013, Pologne (2013a).

Bicking F., **Weber P.**, Theilliol D. Reliability importance measures for fault tolerant control allocation. Dans 2nd International Conference on Control and Fault-Tolerant Systems, SysTol'13 - 2nd International Conference on Control and Fault-Tolerant Systems, SysTol'13, France (2013b).

Fallet G., **Weber P.,** Simon C. Iung B., Duval C. Evidential network-based extension of Leaky Noisy-OR structure for supporting risks analyses. In 8th International Symposium SAFEPROCESS 2012, Mexique, august (2012).

Khelassi A., Theilliol D., **Weber P.,** Zhang Y. Fault-tolerant compensation control incorporating actuator criticality. In 8th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, SAFEPROCESS 2012, Mexico City, Mexique, août (2012).

Weber P., Becker F., Mathias A., Theilliol D., Zhang Y. Reliability analysis of fault tolerant wind energy conversion system with doubly fed induction generator. In 5th International Conference on Intelligent Robotics and Applications, ICIRA 2012 , Montréal, Canada, octobre (2012). Published in Intelligent Robotics and Applications , Lecture Notes in Computer Science, Volume 7506, pp 483-492, (2012c).

Weber P., Simon C., Theilliol D., Puig V. Fault-tolerant control design for over-actuated system conditioned by reliability: a drinking water network application. In 8th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, SAFEPROCESS 2012, Mexico City, Mexique, août (2012d).

Khelassi A., Theilliol D., **Weber P.,** D. Sauter. A novel active fault tolerant control design with respect to actuators reliability. 50th IEEE Conference on Decision and Control and European Control Conference, Orlando : Florida - USA, December 12-16 (2011a).

Khelassi A., Theilliol D., **Weber P.,** Ponsart J.C. Fault-tolerant control design with respect to actuator health degradation: An LMI approach. IEEE Conference on Control Applications, Denver : Colorado - USA, September 28-30 (2011b).

Weber P., Simon C., Theilliol D., Puig V. Control allocation of k-out-of-n systems based on Bayesian Network Reliability model: Application to a drinking water network. ESREL 2011 Annual Conference, Troyes, France, September 18-22 (2011).

Khelassi A., J. Jiang, Theilliol D., **Weber P.,** Zhang Y. Reconfiguration of Control Inputs for overactuated Systems based on Actuators health. 18th IFAC World Congress, Milan: Italy, August 29- September 02 (2011c).

Khelassi A., **Weber P.,** Theilliol D., Aubrun C. Evaluation of Fault Tolerant System against Actuators Aging applied to Flotation Circuit. 18th IFAC World Congress, Milan: Italy, August 29- September 02 (2011d).

Fallet G., Duval C., Simon C., **Weber P.,** Iung B. Expert judgments collecting and modeling: Application to the Integrated Risks Analysis (IRA) methodology. 3rd International Workshop on Dependable Control of Discrete Systems (DCDS), Saarbrucken : Deutschland, June, (2011), 72–77. DOI: 10.1109/DCDS.2011.5970321

Weber P., Simon C., Theilliol D. Reconfiguration of over-actuated consecutive-k-out-of-n: F systems based on Bayesian Network Reliability model. 8th Workshop on Advanced Control and Diagnosis, Ferrara: Italy, November (2010).

Khelassi A., **Weber P.,** Theilliol D. Reconfigurable Control Design for over-actuated Systems based on Reliability Indicators, Conference on Control and Fault-Tolerant Systems, Nice : France, October, (2010a), 365-370.

Khelassi A., Theilliol D., **Weber P.** Control Design for Overactuated Systems based on Reliability Indicators. UKACC International Conference on Control, Coventry : UK, September (2010b).

Medina-Oliva G., **Weber P.,** Levrat E., Iung B. Use of probabilistic relational model (PRM) for dependability analysis of complex systems. 12th IFAC Symposium on Large Scale Systems: Theory and Applications, LSS 2010, Villeneuve d'Ascq : France, (2010).

Fallet G., Duval C., **Weber P.,** Simon C. Characterization and propagation of uncertainties in complex socio-technical system risk analyses. 1st international Workshop on the Theory of Belief Functions, Brest: France, (2010).

Medina-Oliva G., **Weber P.,** Levrat E., Iung B. Probabilistic relational model (PRM) based technical knowledge formalization for dependability of an industrial system. 7th Workshop on Advanced Control and Diagnosis, Zielona Gora: Poland (2009b).

Khelassi A., Theilliol D., **Weber P.** Reconfigurability analysis for reliable fault-tolerant control design. 7th Workshop on Advanced Control and Diagnosis, Zielona Gora : Poland, November (2009a).

Khelassi A., Theilliol D., **Weber P.** On reconfigurability for actuator faults under reliability constraints. IFAC Workshop on Automation in Mining, Mineral and Metal Processing, Vina del Mar : Chile, October (2009b).

Theilliol D., Chamseddine A., Zhang Y., **Weber P.** Optimal reconfigurable control allocation design based on reliability analysis. 7th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, Barcelona : Spain, June 30- July 3 (2009).

Verron S., **Weber P.,** Theilliol D., T. Tiplica, A. Kobi, C. Aubrun. Decision with Bayesian network in the concurrent faults event. 7th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, Barcelona: Spain, June 30- July 3 (2009).

Theilliol D., A. Chamseddine, Y. Zhang, **Weber P.** Design of actuator reconfigurable control allocation versus reliability analysis. 6th Workshop on Advanced Control and Diagnosis, Coventry : UK, November 27-28, (2008), 327-332.

Léger A., R Farret, Duval C., Levrat E., **Weber P.,** Iung B. A safety barriers-based approach for the risk analysis of socio-technical systems. IFAC World Congress 17 (1), Coex : Korea, South, (2008a), 6938-6943.

Weber P., P. Poure, Theilliol D., Saadate S. Design of Hardware Fault Tolerant Control Architecture for Wind Energy Conversion System with DFIG based on Reliability Analysis. IEEE International Symposium on Industrial Electronics, Cambridge : UK, June 30 – July 2, (2008).

Léger A., Duval C., R. Farret, **Weber P.,** Levrat E., Iung B. Modeling of human and organizational impacts for system risk analyses. 9th International Probabilistic Safety Assessment and Management Conference, PSAM 9, Hong Kong, (2008b).

Verron S., **Weber P.,** Theilliol D., T. Tiplica, A. Kobi, C. Aubrun. Using Bayesian networks for decision in the simultaneous faults case. 6th Workshop on Advanced Control and Diagnosis, Coventry : UK, November 27-28, (2008).

Duval C., Léger A., **Weber P.,** Levrat E., Iung B., Farret R. Choice of a risk analysis method for complex socio-technical systems. European Safety and Reliability Conference, ESREL 2007, Stavanger, Norvège, 25 July, (2007).

Weber P., Theilliol D., Poure P., Saadate S. Reliability analysis in a fault tolerant control strategy dedicated to active power filter. Workshop on Advanced Control and Diagnosis, ACD'2006, Nancy, France (2006).

Léger A., Duval C., **Weber P.,** Levrat E., Farret R. Bayesian Network Modelling the risk analysis of complex socio technical systems. Workshop on Advanced Control and Diagnosis, ACD'2006, Nancy, France (2006).

Weber P., Theilliol D., Aubrun C., Evsukoff A.G. Increasing effectiveness of model-based fault diagnosis: A Dynamic Bayesian Network design for decision making. 6th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, Beijing, P.R. China, 30 august, (2006), pp. 109-114.

Ben Salem A., Muller A., **Weber P.** Dynamic Bayesian Networks in system reliability analysis. 6th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, Beijing, P.R. China,30 august, (2006), pp. 481-486.

Guenab F., Theilliol D., **Weber P.,** Ponsart J.C., Sauter D. Fault-tolerant control design based on cost and reliability analysis. 16th IFAC World Congress, Prague, Czech Republic, Juillet 4 – 8, (2005).

Guenab F., Theilliol D., **Weber P.,** Ponsart J.C., Sauter D. Fault-tolerant control design based on cost and reliability analysis. Workshop on Advanced Control and Diagnosis (ACD), Karlsruhe, Germany, November 17 - 18, (2004b).

Bouillaut L., **Weber P.,** Ben Salem A., Aknin P. Use of Causal Probabilistic Networks for the improvement of the Maintenance of Railway Infrastructure. IEEE International Conference on Systems, Man and Cybernetics, Hague, Netherlands, October 10-13, (2004).

Muller A., **Weber P.,** Ben Salem A. Process model-based Dynamic Bayesian Networks for Prognostic. IEEE 4th International Conference on Intelligent Systems Design and Applications, Budapest, Hungary, August 26-28, (2004).

Ben Salem A., Bouillaut L., Aknin P., **Weber P.** Dynamic Bayesian Networks for classification of rail defects. IEEE 4th International Conference on Intelligent Systems Design and Applications, Budapest, Hungary, August 26-28, (2004).

Weber P., Munteanu P., Jouffe L. Dynamic Bayesian Networks modelling the dependability of systems with degradations and exogenous constraints. 11th IFAC Symposium on Information Control Problems in Manufacturing, INCOM'04. Salvador-Bahia, Brazil, April 5-7th, (2004).

Weber P., Jouffe L. Reliability modelling with Dynamic Bayesian Networks. 5th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes (SAFEPROCESS'03), Washington, D.C., USA, June 9-11, (2003).

Weber P. Dynamic Bayesian Networks model to estimate process availability. 8th International Conference Quality, Reliability, Maintenance, CCF'02. Sinaia, Romania (2002).

Weber P, Suhner MC. An application of Bayesian Networks to the performance analysis of a process. In : Proceedings of lm 13, ESREL 2002 European conference. Lyon, France, (2002).

Weber P., Suhner M.C., Iung B. System approach-based Bayesian Network to aid maintenance of manufacturing process. 6th IFAC Symposium on Cost Oriented Automation, Low Cost Automation, Berlin, Germany, 8-9 Oct., (2001a).

Weber P., Suhner M.C. System architecture design based on a Bayesian Networks method. Xth Internationnal Symposium on Applied Stochastic Models and Data Analysis, Compiègne, France, June 12-15, (2001b).

Weber P., Gentil S., Barraud A. On-line forgetting factor adaptation for parameter estimation based diagnosis. IFAC/IFIP/IEEE, Second Conference on Management and Control of Production and Logistics (MCPL 2000), Grenoble, France, 5-8 Juillet, (2000), (6 pages).

Weber P., Gentil S., Ripoll P., Foulloy L. Multiple fault detection and isolation. 14th IFAC World Congress, Vol.P, pp 223-228, Beijing, China, (1999).

Weber P., Gentil S. A parameter estimation method for the diagnosis of sensor or actuator abrupt faults. ECC99, support CD-ROM, Karlsruhe, Germany, (1999), (6 pages).

Evsukoff A., **Weber P.**, Gentil S. Decision procedures for fault detection and isolation derived from knowledge and data. ECC99, support CD-ROM, Karlsruhe, Germany, (1999), (6 pages).

Weber P., Gentil S. Fault detection and isolation using Multiple model parameter estimation. CESA'98 IMACS, Multiconference, Computational Engineering in Systems Applications, Vol.3, pp 467-472, Nabeul-Hammamet, Tunisia, Apr. 1-4, (1998).

Weber P., Gentil S. Fault detection using parameter estimation applied to a winding machine. IAR Annual Conference, Duisburg, Allemagne, Nov. 20-21, (1997), (6 pages).

Theilliol D., **Weber P.,** Ghetie M., Noura H. A hierarchical fault diagnosis method using a decision support system applied to a chemical plant. IEEE International Conference on Systems, Man, and Cybernetics, Vol.3, pp 2205-2210, Vancouver, Canada, Oct. 22, (1995).

Conférences nationales ou sans acte (25)

Flacke N., Margaria T., Floyd B., Duerr Specht M., Seemann Monteiro M., Halpern P., De Iaco F., Garcia Castrillo Riesgo L., Wazzan A., **Weber P.,** Barletta C., Bellou A. Managing Knowledge in Emergency Care Technology. DGINA'14 in Nuremberg on November 6th (2014).

Weber P., Simon C., Theilliol D., Puig V. Aide à la décision pour la commande de système sur-actionné tolérant aux défaillances basé sur la fiabilité. Journée ISA France sur la Surveillance des procédés industriels : algorithmes de traitement et aides à la décision-Nancy, 17 octobre (2013).

Simon C., **Weber P.,** Bicking F. Session Didactique : Quelques applications en fiabilité. Journée IMdR- SdF & RUFEREQ sur le thème : « Réseaux Bayésiens : Méthodes et applications à la sûreté de fonctionnement et à la maîtrise des risques », Paris (France), 20 septembre (2012).

Weber P., Simon C. Introduction aux Réseaux Bayésiens et modélisation de la fiabilité. Journée IMdR-SdF & RUFEREQ sur le thème : « Réseaux Bayésiens : Méthodes et applications à la sûreté de fonctionnement et à la maîtrise des risques », Paris (France), 20 septembre (2012).

Weber P., Simon C., Theilliol D., Aubrun C. Bayesian networks to Reliability modeling: applications to fault Diagnosis and Reconfiguration. Journée du GT *ARC-GDR MACS*, ConecsSdF, Paris (France), 27-Jan (2011).

Weber P., Simon C., Theilliol D., Puig V. Allocation de commande pour un système de redondance k/n, basée sur un modèle. 4ème Workshop du Groupement d'Intérêt Scientifique "Surveillance, Sûreté, Sécurité des Grands Systèmes", France (2011).

Medina-Oliva G., **Weber P.,** Levrat E., Iung B. Use of Bayesian Networks (BN) to Asses Maintenance Strategies of Complex Systems Doctoral Spring Workshop “Product and Asset Lifecycle Management” (PALM - DSW), Rosière : France, (2011a).

Medina-Oliva G., **Weber P.,** Iung B. Modélisation, à base de Réseaux Bayésiens, d'un système de maintenance industriel et de son environnement pour l'évaluation de ses stratégies de maintenance. 4èmes Journées Doctorales / Journées Nationales MACS, JD-JN-MACS, Marseille : France (2011b).

Medina-Oliva G., **Weber P.,** Levrat E., Iung B. Probabilistic Relational Model (PRM) based Technical Knowledge Formalization for Maintenance Strategy Assessment of Industrial Systems. Doctoral Spring Workshop “Product and Asset Lifecycle Management” (PALM - DSW), Seville : Espagne (2010).

Khelassi A., Theilliol D., **Weber P.** Synthèse d'une loi de commande reconfigurable assurant la fiabilité des systèmes. Sixième Conférence Internationale Francophone d'Automatique, CIFA, Nancy : France (2010).

Simon C., Bicking F., **Weber P.** Un nouvel outil d'évaluation de la fiabilité : les réseaux de fonctions de croyance. 16ème Colloque National de la Recherche en IUT, CNRIUT - 16ème Colloque National de la Recherche en IUT, CNRIUT, France (2010).

Duval C., Léger A., Farret R., **Weber P.** Méthodologie d’analyse de risques pour les systèmes socio-techniques complexes et application à un cas industriel. 16e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Lambda Mu 16, Avignon : France (2008).

Simon C., **Weber P.,** Aubry JF. Fiabilité imprécise par les réseaux de fonctions de croyance. 16e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Lambda Mu 16, Avignon : France (2008).

Jehl JP., **Weber P.,** Theilliol D., Didier B. L'analyse de non-conformité par plans d'expérience et réseaux Bayésiens : application au surmoulage. 5ème Conférence Internationale Francophone d'Automatique, CIFA'2008, Bucarest : Roumanie (2008).

Simon C., **Weber P.** Fiabilité et performance imprécises des systèmes par les réseaux de fonctions de croyance. Workshop Surveillance, Sûreté et Sécurité des Grands Systèmes, 3SGS'08, Troyes : France, (2008).

Simon C., **Weber P.** Analyse de la fiabilité imprécise des systèmes par les réseaux de fonctions de croyance. 4ème Journées Francophone sur les Réseaux Bayésiens, Lyon : France (2008).

Simon C., **Weber P.,** Aubry JF. Des sous-ensembles flous aux fonctions de croyance: quelques applications pour les systèmes instrumentés de sécurité. Journée de l'institut de Maîtrise Des Risques (IMdR-SdF) sur les nouvelles théories de l'incertain, Paris : France, 17 Septembre (2008).

Weber P. Réseaux bayésiens et applications en fiabilité et maintenance. Journée du GT S^3-*GDR MACS*, fiabilité des systèmes dynamiques, Paris (France), 31 janvier (2008).

Weber P. Evaluation de la fiabilité par réseaux bayésiens. *Journée INTERREG3*, Comment évaluer la performance de vos installations ? Nancy (France), 16 Nov. (2005).

Weber P. Modélisation de la fiabilité d’un système de chauffage complexe (Intérêt des réseaux bayésiens relativement aux méthodes de SdF). Journée IMdR-SdF, Retour d’expérience : les réseaux bayésiens, outils d’analyse et de structuration. Paris (France), 29 Sep. (2005).

Ben Salem A., Bouillaut L., Aknin P., **Weber P.,** Iung B. Réseaux Bayésiens Dynamiques pour la classification d’évènements organisés en séquences temporelles. Journées Doctorales Modélisation, Analyse et Conduite des Systèmes dynamiques, JDMACS 2005, Lyon, France, 5-7 septembre (2005).

Guenab F., **Weber P.,** Theilliol D. Système tolérant aux défauts : reconfiguration et/ou restructuration basée sur la fiabilité et le coût. Journées Doctorales, Nationales du GDR MACS, Lyon (France), du 5 au 7 sep. (2005).

Cerisier L., **Weber P.** Modèle de type réseau bayésien pour l'estimation de la fiabilité des procédés. ***Session invitée,*** 5° Congrès international pluridisciplinaire Qualité et Sûreté de Fonctionnement, Qualita'03, Nancy, 18 mars, (2003).

Weber P. RB et sureté de fonctionnement. 2ème Journée de Rencontre Française sur les Réseaux Bayesiens, Rouen - Madrillet, 7 Mars, (2003).

Weber P., Suhner M.C. Aide au choix de stratégie de maintenance par simulation de réseaux bayésiens. Qualita'01, Annecy, 22-23 Mars, (2001), (6 pages).

Rapports et Notes internes du CRAN (14)

Duval C., Fallet-Fidry G., Iung B., Simon C., Weber P. Maîtrise et Analyse des Risques des systèmes intégrAnt les domaines Techniques, Humains, Organisationnels et enviroNnementaux : Application au domaine de la production électrique, janvier (2012). Rapport du projet MARATHON financé par le GIS 3SGS.

Medina-Oliva G., Iung B., **Weber P.** Formalisation et intégration des connaissances d'un système industriel. Rapport du projet SKOOB, ANR PROJET 07 TLOG 021, (2009b).

Medina-Oliva G., **Weber P.,** Iung B., Levrat E., Simon C. Outils de représentation des différents points de vue d'un système industriel. Rapport du projet SKOOB, ANR PROJET 07 TLOG 021, (2009c).

Medina-Oliva G, **Weber P.,** Iung B., Levrat E., Simon C. Cahier des charges fonctionnel d'un outil d'évaluation des stratégies de maintenance. Rapport du projet SKOOB, ANR PROJET 07 TLOG 021, (2008).

Weber P., Simon C., Medina-Oliva G. Analyse des références en RB/MdR-SdF: 7000 références sur les 10 dernières années. Rapport du projet SKOOB, ANR PROJET 07 TLOG 021, (2008).

Simon C., **Weber P.** Réseaux Bayésiens et Incertitudes. Rapport du projet SKOOB, ANR PROJET 07 TLOG 021, (2008).

Weber P., Joly A., Simon C. MARKOV DECISION PROCESS: Utilisation des processus de décision markoviens pour l'organisation de la maintenance. Rapport du projet SKOOB, ANR PROJET 07 TLOG 021 (2008).

Munteanu P., Clerc C., Suhner M.C., **Weber P.** Projet IMdR P04-7 « Réseaux bayésiens et retour d'expérience en sûreté de fonctionnement », Tâche 3 – Elaboration de recommandations méthodologiques, Septembre (2007).

Munteanu P., Clerc C., Suhner M.C., **Weber P.** Projet IMdR P04-7 « Réseaux bayésiens et retour d'expérience en sûreté de fonctionnement », Tâche 2 – Adaptation spécifique aux EPSdF, Septembre (2007).

Munteanu P., Clerc C., Suhner M.C., **Weber P.** Projet IMdR P04-7 « Réseaux bayésiens et retour d'expérience en sûreté de fonctionnement », Tâche 1 – Etat de l'art, Septembre (2007).

Iung B., Levrat E., Suhner M., **Weber P.,** Voisin A. Rapport de fin de phase 5 ETAT DE L'ART / VEILLE EN E-MAINTENANCE EN GENERAL. Rapport de fin de contrat APIP Besançon, Contrat de sous-traitance APIP 2005 pour une prestation en "Etude d'un système "e-Maintenance" adapté à un système de combat naval", n° 05-024, juin (2005).

Weber P., Iung B., Levrat E., Voisin A. PROJET IDAFH, Analyse d'une approche de modélisation par Réseaux Bayésiens. Rapport de fin de contrat EDF, UHP UNI/2004/044, mai (2005).

Weber P. Projet IDAFH, premier rapport de contrat EDF/CRAN-UHP. Rapport EDF, Contrat de collaboration, n° UINI/2004/044, janvier (2005).

Weber P., Suhner M.C., Iung B. System approach-based Bayesian Network to aid maintenance of manufacturing process. Note Interne du Thème CSSF n° 11_n001, (2001).

Notes internes du LAG (3)

Weber P. Suivi paramétrique pour la surveillance d'installations complexes - rapport de 1ère année. Note interne n° 98.002, Laboratoire d'Automatique de Grenoble, Janvier (1998), (89 pages).

Weber P. Diagnostic de défaut par estimation paramétrique – Analyse des méthodes Erreur d'équation et Erreur de Sortie. Note interne n° 98.181, Laboratoire d'Automatique de Grenoble, Décembre (1998), (66 pages).

Weber P. Diagnostic de défaut par estimation paramétrique – Estimation paramétrique dédiée à la reconnaissance des fonctions de sensibilité d'un résidu d'erreur de sortie pour la localisation de défauts additifs brutaux. Note interne n° 99.026, Laboratoire d'Automatique de Grenoble, Février (1999), (31 pages).

Rapports de DEA (2)

Weber P. Conception et Application d'un Outil de Diagnostic de Défauts Capteurs. Rapport de recherche de DEA, Nancy, (1995), (53 pages).

Weber P. *Système expert temps réel appliqué au diagnostic* Rapport Bibliographique de DEA, Nancy, (1995), (29 pages).

Chapitre 2

Présentation des activités d'enseignement et d'administration

1 Introduction

Depuis ma nomination au poste de maître de conférences à l'Ecole Supérieure des Sciences et Technologies de l'Ingénieur de Nancy (ESSTIN), j'ai pris en charge des enseignements répartis sur chaque année de Bac+1 à Bac+5, (niveau L et M). J'interviens également dans la formation Master en Ingénierie des Systèmes Complexes (ISC) de l'UL, en cours et en encadrement de projets et de stages master ainsi que dans le co-encadrement des doctorants de l'École Doctorale IAEM Lorraine (niveau D). Ces enseignements : de cours, de travaux dirigés, et de travaux pratiques ainsi que l'encadrement de projets, de stages et de doctorats m'ont permis de côtoyer des étudiants de tous les niveaux.

Depuis ma titularisation, ma volonté est de relier mes activités de recherche et d'enseignement. J'ai donc progressivement pris la responsabilité des enseignements en maintenance, en sûreté de fonctionnement et en maîtrise des risques pour manager cet axe dans l'Ecole Supérieure des Sciences et Technologies de l'Ingénieur de Nancy (ESSTIN). J'ai fait évoluer les enseignements vers la modélisation de systèmes complexes. Aujourd'hui des outils modernes de modélisation tels que les réseaux bayésiens, les réseaux de fonctions de croyances sont enseignés à l' ESSTIN. J'ai également fait évoluer l'enseignement de la maintenance vers une maintenance moderne intégrant la notion de développement durable et d'innovation.

2 Responsabilités pédagogiques et administratives de formation

Mes responsabilités pédagogiques ont débutées dès mon arrivée à l'ESSTIN :

- 2000-2001 Responsable des TP en Electronique et Informatique Industrielle (Automates Programmables), 3ème année ESSTIN ; écriture des sujets de 5 nouveaux TP.

- 2001-2009 Responsable des TP en Technologie de 2ème année ESSTIN, rebaptisés en 2003 Composants Technologiques ; mise aux normes, écriture des sujets et réactualisation des platines d'expérimentations.
- 2003 - 2007 Membre du Groupe de Réflexions sur le Programme Pédagogique (GRPP) de l'ESSTIN.
- 2004 - 2005 Responsable de l'option ESSTIN - Maintenance Industrielle (MI).
- 2005 - 2008 Responsable des relations industrielles, des projets et stages de l'option ESSTIN - Maintenance Industrielle (MI).
- 2008 - 2010 Responsable pédagogique de l'option ESSTIN - Maintenance Industrielle (MI).
- Depuis 2011 Responsable pédagogique de l'option ESSTIN - Maintenance et Sûreté des Systèmes (MSS).
- Depuis 2012 Responsable des contrats de professionnalisation de l'option ESSTIN - Maintenance et Sûreté des Systèmes (MSS).
- 2014 – 2015 : Animateur de la réflexions sur le programme pédagogique du diplôme orienté : maintenance, développement durable, maîtrise des risques, et management de l'innovation de Polytech Nancy.

Mon implication forte au sein des tâches d'animation de formations a débuté en 2004 en tant que responsable de l'option de fin d'études : Maintenance Industrielle (MI) (Figure 3). Cette implication me permet d'établir une cohérence entre mes travaux de recherche et mes activités d'enseignements.

Après une première année comme responsable pédagogique de l'option MI, j'ai poursuivi avec la responsabilité des projets, des stages et les relations industrielles de l'option MI de 2005-2008. Enfin, j'ai repris la responsabilité pédagogique de l'option MI en 2008, accompagné de Luc Lossent sur la partie projets et stages. J'ai malheureusement été contraint d'interrompre cette responsabilité en 2010-2011 pour raison de santé.

<table>
<tr><th></th><th>2004-2005</th><th>2005-2006</th><th>2006-2007</th><th>2007-2008</th><th>2008-2009</th><th>2009-2010</th><th>2010-2011</th><th>2011-…</th></tr>
<tr><td>Responsable Etudes & Pédagogie</td><td rowspan="2">Philippe Weber</td><td colspan="3">Gilles Millerioux</td><td colspan="2">Philippe Weber</td><td rowspan="2">Luc Lossent</td><td>Philippe Weber</td></tr>
<tr><td>Responsable Projets & Stages</td><td colspan="3">Philippe Weber</td><td colspan="2">Luc Lossent</td><td>Luc Lossent</td></tr>
<tr><td></td><td colspan="4">Option : Maintenance Industrielle (MI)</td><td colspan="4">Option Maintenance et Sûreté de Systèmes (MSS)</td></tr>
<tr><td>Association de l'option aux masters</td><td colspan="5"></td><td colspan="3">Master ISC-UL
Master MI-IAE</td></tr>
<tr><td>Professionnalisation</td><td colspan="7"></td><td>Alternance</td></tr>
</table>

Figure 3 : Evolution de la responsabilité pédagogique de l'option MSS.

En 2008 j'ai apporté une nouvelle visibilité à la formation en changeant le nom de l'option Maintenance Industrielle (MI) qui est devenue : Maintenance et Sûreté des Systèmes (MSS). J'ai orienté le programme pédagogique pour donner plus d'importance aux cours en lien avec les domaines de la sûreté de fonctionnement et de l'analyse des risques pour rester concurrentiel parmi les propositions de formations d'ingénieurs et répondre aux besoins industriels notamment sur la modélisation probabiliste des systèmes complexes.

Dans cette première modification du programme pédagogique, nous avons intégré 4 cours de Master Ingénierie des Systèmes Complexes de l'Université de Lorraine (ISC-UL) dans les

Eléments de Cours (EC) obligatoires de l'option MSS. Ceci permet l'obtention par les étudiants qui le souhaite d'un double diplôme Ingénieur ESSTIN et Master (ISC-UL), Spécialité : Management Intégré de la Production de Biens et de Services. D'un point de vue pédagogique cette modification permet de faire intervenir dans la formation MSS de l'ESSTIN les enseignants nancéens experts en enseignement et en recherche dans les matières de la maintenance et de la sûreté de fonctionnement (B. Iung, D. Theilliol, E. Levrat, C. Simon, F. Bicking, A. Voisin). Nous avons un flux moyen de 25 étudiants diplômés par an.

La prise en compte de l'impact des activités industrielles sur l'environnement et dans l'économie de la société est une évolution transverse à tous les secteurs d'activités. Les métiers d'ingénieurs sont concernés par cette nouvelle façon de penser, par conséquent, ces métiers se transforment et de nouveaux besoins apparaissent. Les ingénieurs doivent avoir des compétences en développement durable, je me suis engagé à développer cet axe dans la formation des ingénieurs MSS. En 2011, j'ai fait évoluer le programme pédagogique pour renforcer l'adéquation avec les normes sur le développement durable. J'ai mobilisé les enseignants pour réorienter le programme pédagogique de leur EC en cohérence avec le grenelle de l'environnement et l'adossement des enseignements aux normes : ISO 9000, ISO 14000, ISO 26000, ISO 30000 …

Nous proposons, depuis 2011, avec Elise Marcandella (MdC au CEREFIGE-UL), un cours sur l'analyse des normes de la maintenance et leur modification pour les rendre conformes à la notion de développement durable.

- Maintenance, un levier de la soutenabilité des systèmes (MSo), 5ème année (ESSTIN), depuis 2011 ; Enseignant : Elise MARCANDELLA et Philippe WEBER ; volume horaire : 12h CM ; 8hTP.

Dans ce cours, le problème de décision en maintenance pour la formalisation de plans de maintenance ou la définition de procédures de maintenance est examiné en relation avec l'évaluation d'indicateurs de soutenabilité du système. Ceci a pour effet de poser le problème de hiérarchisation des solutions par rapport à leurs impacts économiques, environnementaux, sociaux et sociétaux. Ce cours donne des clefs qui permettront aux ingénieurs de contribuer à un pilotage du service maintenance à des fins d'amélioration de la soutenabilité du système ainsi qu'à une meilleure prise en compte de l'obsolescence.

C'est une orientation originale que notre école a choisi de mettre en avant par la création d'un diplôme orienté : « maintenance, développement durable, maîtrise des risques, management de l'innovation » pour l'intégration de l'ESSTIN dans le réseau Polytech. Je suis animateur des réflexions sur la formalisation du programme pédagogique de ce nouveau diplôme, pour le prochain passage de la Commission des Titres d'Ingénieurs (CTI).

Je suis, depuis 2008, responsable de l'option MSS. Cette implication m'a permis, en étant à l'écoute des industriels, d'orienter mes activités de recherche sur les problèmes de l'aide à la décision en maintenance et de la modélisation probabiliste en sûreté de fonctionnement. Mes travaux de recherche m'ont permis d'alimenter les cours et ainsi d'assurer un transfert des connaissances vers les ingénieurs ESSTIN. Nous avons un flux moyen de 25 étudiants diplômés par an. Dans le cadre de cette responsabilité d'option mes tâches sont aussi la gestion des relations avec les entreprises pour assurer un vivier de propositions de stages et

un potentiel d'embauche de nos étudiants (en 2014, 70% des ingénieurs ESSTIN-MSS ont signé un CDD ou CDI avant l'obtention du diplôme). Ceci est rendu possible par le suivi de stages d'ingénieurs qui me permet un contact direct avec les responsables industriels, ainsi que les contacts que je maintiens avec les anciens élèves de l'option MSS à travers les réseaux de relations professionnelles (Viadéo et LinkedIn).

L'élaboration des emplois du temps est une tâche qui n'est pas toujours facile compte tenue qu'aujourd'hui, l'option MSS est synchronisée avec deux formations de master : le Master Ingénierie de Systèmes Complexes (ISC-UL) et le Master Management de l'Innovation (MI-IAE Metz). De plus, depuis 2012, une partie des étudiants choisissent une formation en alternance (en contrat de professionnalisation sur 1 an). Il est donc nécessaire d'organiser les emplois du temps pour leur permettre de suivre la totalité des EC de l'option MSS sans aucune différence avec le reste de la promotion.

Dans cette option, les intervenants sont soit des enseignants de l'ESSTIN (36%) ; soit des enseignants d'autres composantes de l'Université de Lorraine (25%) ; soit des industriels (39%) (Figure 4). Les enseignements sont répartis sur plusieurs sites : ESSTIN, AIPL, (ENSAIA et IAE Metz pour le master MI-IAE Metz).

Je m'attache également à la centralisation des supports numériques de tous les cours des intervenants extérieurs ; à la gestion de la plateforme de diffusion des cours ; à l'élaboration des relevés de notes et PV de jury ; à l'organisation des sessions de rattrapage ; à la réalisation de la plaquette d'information, du syllabus et à la présentation des enseignements de l'option MSS.

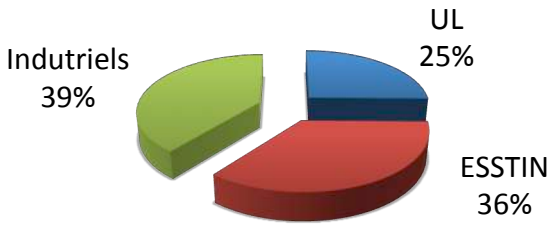


Figure 4 : Origine des intervenants de l'option MSS

3 Profil de mes enseignements et liens avec mes travaux de recherche

En moyenne j'effectue 200h équivalent TD d'enseignements annuelles qui se répartissent dans la formation initiale en présentielle pour 46% en CM, 38% en TD et 16% en TP comme l'indique le tableau suivant et la Figure 5.

Titre de l'enseignement	Niv.	Cours	TD	TP
Codage des données 1er année (ESSTIN)	L	12	32	
Maintenance et Sûreté de fonctionnement 4ème année (ESSTIN), Master ISC	M	12	12	
Maintenance Basée sur la Fiabilité et outils technologiques	M	6		8

5ème année (ESSTIN)				
GMAO et Systèmes d'aide au diagnostic 5ème année (ESSTIN)	M	4		8
Systèmes tolérants aux fautes et fiabilité 5ème année (ESSTIN), Master ISC	M	8		
Sûreté de fonctionnement et maîtrise des Risques, 5ème année (ESSTIN), Master ISC	M	20	32	
Maintenance, un levier de la soutenance des systèmes 5ème année (ESSTIN)	M			8
Analyse intégrée des risques 5ème année (ESSTIN)	M			8

A ce service s'ajoutent les encadrements de projets et de stages avec en moyenne, le suivi des 3 étudiants en alternance par an et le suivi de 3 étudiants par an soit en double inscription ESSTIN-MSS et Master ISC, soit en simple inscription ESSTIN-MSS.

Les matières dont j'ai eu la charge relèvent des disciplines de l'EEA. Je suis intervenu dans des enseignements répartis sur tout le cycle d'ingénieur comme l'illustre la Figure 6. L'annexe A présente la liste des documents de cours et sujet de TD et TP que j'ai produit pour mes enseignements à l'ESSTIN.

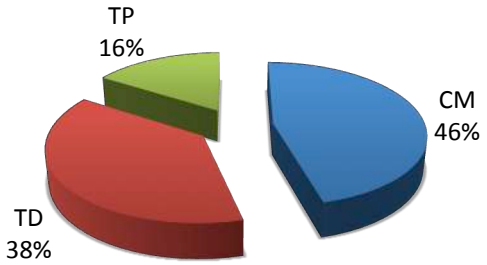


Figure 5 : Répartition de mes activités pédagogiques

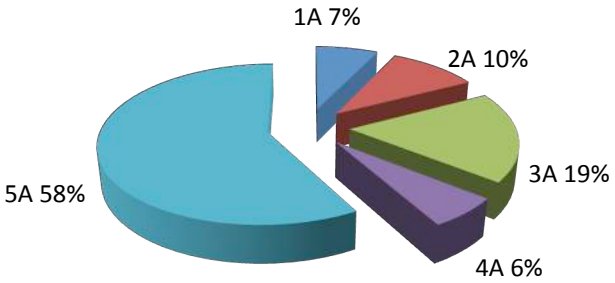


Figure 6 : Répartition de mes activités pédagogiques par année d'étude des étudiants

Je suis responsable des cours :

- Risque et Sûreté des systèmes, 4ème année (ESSTIN), depuis 2013 ; Enseignants : Philippe WEBER, Frédérique BICKING-SIMON; volume horaire : 12h CM, 12hTD.

- Sûreté de fonctionnement et maîtrise des risques (SDF) 5ème année (ESSTIN), depuis 2000 ; Enseignant : Philippe WEBER ; volume horaire : 20h CM, 16h TD ; (ce cours est commun au Master ISC depuis 2008, en visio-conférence avec l'ENS Cachan).
- Maintenance Basée sur la Fiabilité et Outils technologiques pour la maintenance (MBF), 5ème année (ESSTIN), depuis 2003 ; Enseignants : Philippe WEBER, Jean-Michel Guillemot et Joël Mongin; volume horaire : 20h CM, 8hTP.
- GMAO et Système d'aide au diagnostic (GMAO) 5ème année (ESSTIN), depuis 2003 ; Enseignants : Philippe WEBER et Guilhem PATERNOTTE ; volume horaire : 16h CM, 8h TP.
- Systèmes tolérants aux fautes et fiabilité (STF) 5ème année (ESSTIN), depuis 2008 ; Enseignants : Philippe WEBER, Didier THEILLIOL ; volume horaire : 20h CM ; (ce cours est commun au Master ISC depuis 2008).
- Analyse intégrée des risques (AIdR) 5ème année (ESSTIN), depuis 2013 ; Enseignants : Carole DUVAL, Philippe WEBER ; volume horaire : 8h CM, 8hTD.

Mes compétences en maîtrise des risques acquises lors de contrats de recherche avec les ingénieurs experts en recherche et développement de grands groupes industriels et mon expertise sur la modélisation probabiliste par réseaux bayésiens appliquée à la sûreté de fonctionnement me permettent de former des ingénieurs et des étudiants de Master 2 (recherche) sur ces techniques de modélisation en plein essor. Les ingénieurs ESSTIN et les étudiant de Master ISC sont formés pour résoudre des problèmes de modélisation de systèmes complexes. Ils peuvent répondre aux demandes d'embauche en sûreté de fonctionnement. Par exemple j'aborde, dans les cours SDF, STF et AIdR, en plus des méthodes traditionnelles, différentes applications de la modélisation graphique probabiliste en liens avec des systèmes complexes.

4 Encadrement de stages et de projets

J'ai encadré plus de 75 projets réalisés par les étudiants de 5ème année de l'option Maintenance Industrielle puis de l'option Maintenance et Sûreté des Systèmes de la formation d'ingénieur de l'ESSTIN. L'objectif des projets est de former les étudiants à la recherche d'information, l'organisation de leur temps de travail et l'approfondissement de notions abordées en cours. Les sujets que je propose sont soit **en lien avec mes activités de recherche**, soit un **approfondissement des cours** de la formation de 5ème année. Nous avons donc des projets sur les outils de modélisation tels que les réseaux bayésiens, les arbres de défaillance, les chaines de Markov etc. Les projets que je propose permettent de manière cohérente de progresser années après années sur des axes en relation avec la problématique de modélisation de systèmes en sûreté de fonctionnement, et dès que cela est possible je propose aux étudiants de valoriser leur travail à travers des publications. Les applications sont ciblées soit sur des cas d'école pour des outils de modélisation novateurs par exemple :

Kulik M. : Chaîne de Markov appliquée à la modélisation probabiliste du processus de stockage d'un composant, 2004.

Jung M. : Modélisation et simulation de systèmes sous BayesiaLab pour la recherche de stratégies de maintenance (Système à 3 vannes), 2005. **Ce travail a donné lieu à une diffusion sur le site internet de Bayesia : www/bayesia.com**

Gautier F. : Pronostic de fiabilité du système en pont avec incertitude paramétrique, par réseau de fonction de croyance dynamique, 2006. **Ce travail a donné lieu à un article de conférence : MED 2008.**

Soit sur des cas concrets comme par exemple :

Mathias A. : Sûreté de fonctionnement d'un système de production d'énergie par éolienne (analyse par chaîne de Markov de la fiabilité d'un système de commande tolérante aux défauts), 2011. **Ce travail a donné lieu à un article de conférence : ICIRA 2012**.

Agnes T. : Analyse de sûreté de fonctionnement d'un réseau de distribution d'eau potable (génération automatique d'un modèle réseaux bayésien), 2011.

Carpentier A. : Evaluation probabiliste de l'efficacité de barrières humaines, maîtrise des risques en production d'énergie EDF, 2013.

Enfin, j'ai encadré 8 étudiants en alternance et plus 60 stages de fin d'études d'ingénieur maintenance et sûreté des systèmes. Les stages ingénieurs permettent aux étudiants de valoriser leurs acquis dans un contexte industriel. Les secteurs d'activités sont très variés : agroalimentaire, chimie, production d'énergie (pétrole, gaz, nucléaire), métallurgie, militaire, exploitations offshore, pharmaceutique, santé, transports (aérien, spatial, routier, ferroviaire, maritime). Cette vision large du milieu industriel dans les domaines de la maintenance et de la sûreté de fonctionnement est très enrichissante et me permet de relever les difficultés rencontrées par les industriels et alimente soit mes cours si les difficultés peuvent être résolues avec les méthodes que j'enseigne ou mes activités de recherche si les problèmes sont plus complexes et nécessitent des développements plus poussés.

5 Enseignement hors ESSTIN

Les connaissances et les nouvelles méthodes et outils que nous développons en recherche doivent être diffusés le plus largement possible. J'ai donc participé à différents cours dans cet esprit de 2002 à 2009. Je remercie François Pérès qui m'a invité à l'Ecole Centrale Paris, Jean François Aubry qui m'a invité à l'ENSEM ainsi que Luis Gerardo Vela Valdes qui m'a invité au centre de recherche Centro Nacional de Investigación y Desarrollo Tecnológico (CENIDET), Cuernavaca, Morelos, MEXIQUE.

6 Conclusion

J'ai orienté mes activités d'enseignements pour qu'elles restent complémentaires à mes activités de recherches.

Je participe à la formation de master (recherche), cela me permet de détecter des étudiants, soit de master, soit en double inscription en école d'ingénieur et en master, capables de poursuivre leurs études vers une formation doctorale.

Je suis, par mes responsabilités d'option de fin d'étude, moteur dans l'élaboration des programmes pédagogiques. Cela me permet d'infléchir les orientations de la formation, en accord avec la demande du marché de l'emploi des ingénieurs en maintenance et en sûreté

de fonctionnement, mais aussi, en intégrant des méthodes pertinentes pour la résolution des problèmes de modélisation en maîtrise des risques industriels.

Mes relations avec le monde industriel alimentent mes recherches et orientent le programme pédagogique de la formation ESSTIN option MSS. Les étudiants sortants de l'option MSS (25 diplômés par an en moyenne) sont embauchés à 70% avant l'obtention de leur diplôme.

J'oriente depuis quelques années la formation de l'option MSS vers le développement durable. C'est une orientation que notre école a choisie de mettre en avant par la création d'un diplôme : « Maintenance, Développement durable, Maîtrise des risques, Management de l'innovation » pour l'intégration de l'ESSTIN dans le réseau Polytech.

Chapitre 3

Présentation des activités de recherche

1 Introduction

Le défi scientifique de mes travaux de recherche est de formaliser des méthodes de construction des modèles probabilistes du fonctionnement et du dysfonctionnement d'un système industriel. Ces modèles ont pour but de permettre l'évaluation des objectifs de fonctionnement du système (exigences opérationnelles, performances) et les conséquences de l'exploitation du système en terme de fiabilité et de maîtrise des risques (exigences de sûreté). Cette représentation nécessite la modélisation des impacts de l'environnement sur le système et sur ses performances, mais il est aussi nécessaire de modéliser l'impact des stratégies de commande et des stratégies de maintenance sur l'état de santé du système.

Cette activité de recherche répond à une problématique industrielle : l'ingénieur doit maintenir et optimiser en continu la qualité des services délivrés par les objets industriels qu'il exploite. Pour cela, il doit disposer de modèles permettant d'évaluer l'impact des actions de maintenance ou de conduite sur le maintien en conditions opérationnelles du système et ainsi l'aider dans la prise de décisions. Malheureusement, la plupart des ingénieurs n'ont pas les méthodes de modélisation pour simuler les systèmes en intégrant les contraintes opérationnelles et les perturbations qui conditionnent leur fonctionnement.

Il est bien souvent impossible de connaître exactement l'état du système avant de prendre une décision, car l'état des composants n'est, en général, pas directement ou instantanément observable. La décision va donc porter sur le pronostic du fonctionnement à venir du système. Cette perception imparfaite est en faveur de l'utilisation d'une évaluation probabiliste de l'état du système.

La classe des modèles considérés dans mes activités de recherche repose sur des modèles probabilistes. Ces modèles sont construits par expertise et par l'analyse de formalisme de représentation métier de différentes natures (AMDEC, HAZOP, SADT). Nous faisons l'hypothèse que les données disponibles ne sont pas suffisantes ou ne représentent pas les informations nécessaires pour la construction du modèle par des algorithmes d'apprentissages automatiques.

Nous proposons dans la suite de ce document d'exposer quelques principes de structuration des connaissances qui permettent de garantir un modèle de sûreté de fonctionnement valide et qui illustrent notre démarche scientifique de formalisation des méthodes de construction de modèle exploitant la flexibilité et l'efficacité de la représentation par modèles graphiques probabilistes. La suite de ce chapitre est divisée en 5 parties :

- La section 2 présente la capacité de modélisation d'un réseau bayésien et illustre sur un exemple la représentativité de ce formalisme de modélisation qui en fait une méthode adaptée au problème de modélisation des systèmes multi-états en sûreté de fonctionnement.

- La section 3 introduit les principes de construction d'un modèle par RB en sûreté de fonctionnement. Il existe plusieurs représentations d'un même problème, nous montrons les liens entre les représentations en partant de l'exemple de la section 2. C'est sur ces principes que repose la formalisation des méthodes de construction des modèles développés dans les thèses de A. Léger (2009), G. Fallet (2012), G. Oliva-Medina (2011) et le projet ANR (SKOOB, 2011).

- La section 4 présente l'intégration de la dimension temporelle dans la modélisation par Réseaux Bayésiens Dynamiques (RBD). Cette partie fait le lien entre différents modèles de processus stochastiques et décrit la représentation élégante que permet un RBD de la fiabilité des composants. Cette section termine sur la complexité de la modélisation et les difficultés auxquelles les algorithmes d'inférence font face lors de la fusion des connaissances à un niveau système. Ce qui permet de comprendre les limites de l'approche et le travail restant à réaliser. La modélisation par RBD est la solution que nous avons retenue dans les travaux de thèse de A. Ben Salem (2008) pour répondre à un problème de diagnostic.

- La section 5 présente une application originale de la modélisation de la fiabilité des systèmes par RBD appliquée à une problématique de commande de système continu. Cette section prend appui sur les travaux développés dans les thèses de F. Guenab (2007) et A. Khelassi (2011). C'est une activité de recherche en cours de développement dont les premiers résultats sont très prometteurs.

- Enfin la section 6 conclue ce chapitre en énonçant mes différentes contributions en dégageant les trois apports majeurs à la communauté scientifique de mon travail de recherche.

2 Réseaux Bayésiens : un formalisme de modélisation pour la sûreté de fonctionnement

Pour les systèmes complexes qui nous intéressent, il est supposé que le système ainsi que les composants ont un nombre fini d'états ou de niveaux de fonctionnement : le système et les composants sont dits : multi-états. Dans ce cas, l'évaluation de la fiabilité du système devient difficile car elle doit prendre en compte les effets de combinaisons des défaillances qui ne sont pas indépendantes de par la nature multi-état des composants du système. Le résultat est un développement d'une grande quantité de scénarios à modéliser qui devient fastidieux pour l'analyste. Dans ce type de circonstances, les méthodes de modélisation classiques atteignent leurs limites principalement du fait de leurs fondements basés sur la logique booléenne ou nécessitent de nombreuses simulations par tirage aléatoire.

Comme le précise (Boutillier et al., 1999), les méthodes de modélisation de l'Intelligence Artificielle (IA) tels que les Réseaux Bayésiens (RB) peuvent apporter une aide efficace dans la prise de décisions de conduite, de maintenance ou de réduction des risques pour des systèmes industriels. Les RB possèdent un pouvoir de modélisation et d'analyse important. Ils fournissent un cadre formel permettant de manipuler ou traiter des événements probabilistes en les représentant par des variables aléatoires discrètes (Pearl 1988 ; Jensen 1996) ainsi que les relations qui les lient en les représentant par des probabilités conditionnelles. La modélisation par RB est réputée pour être fondée sur un puissant formalisme d'expression des dépendances et indépendances complexes entre des variables aléatoires multi-états. Ce formalisme est donc bien adapté à la représentation de systèmes complexes multi-états.

L'application des RB à la sûreté de fonctionnement est un développement relativement récent, leur popularité a grandi dans le domaine des analyses de fiabilité des systèmes depuis la fin des années 90 (Torres-Toledano et Sucar, 1998 ; Kang et Golay, 1999). Nous avons référencé, dans l'article (Weber et al. 2012), un ensemble de 200 articles dans ce domaine et montré l'intérêt porté à la modélisation par RB dans le domaine de la sûreté de fonctionnement et de l'analyse des risques durant ces dix dernières années.

Les articles marquants se sont attachés à démontrer l'équivalence avec les méthodes d'évaluations probabilistes classiquement utilisées en sûreté de fonctionnement. Nous trouvons dans les travaux de Torres-Toledano (Torres-Toledano et Sucar, 1998) une analyse des avantages des RB par rapport au formalisme des Diagrammes de Fiabilité (DF). Les travaux de Bobbio (Bobbio et al., 2001 et 2003) expliquent comment un Arbre de Défaillance peut être modélisé par un RB. Enfin, (Boudali et Dugan, 2005a, 2005b et 2006 ; Portinale et al. 2010) décrivent la représentation des Arbres de Défaillances Dynamiques par des Réseaux Bayésiens Dynamiques. Nous avons durant cette période travaillé sur le lien avec les techniques de modélisation de la fiabilité des systèmes par Chaînes de Markov comme l'illustrent les articles (Weber 2002, Weber et Jouffe 2003, 2006 ; Ben Salem et al. 2006).

Parallèlement à ces comparaisons de méthodes, de nouvelles méthodes de modélisation qui utilisent les capacités de modélisation des RB sont apparues. L'un des premiers articles (Mahadevan et al., 2001) propose une méthodologie exploitant la modélisation par RB dans le cadre de l'évaluation de la fiabilité d'une infrastructure. Cette méthodologie permet la modélisation de deux caractéristiques importantes des grandes structures : la modélisation de plusieurs séquences de défaillances, et des corrélations entre les états-limites au niveau des composants.

Une grande partie de mes travaux (Muller et al., 2004 ; Leger et al., 2009 ; Medina-Oliva et al., 2013 et 2015) est focalisée sur la proposition d'une nouvelle démarche de construction et de justification d'un modèle RB pour l'analyse de la fiabilité ou l'analyse des risques de systèmes complexes. La publication récente de Bensi et al. (2013) propose une méthode de

construction de la structure du modèle RB défini en fonction de liens minimum ou des coupes minimales, pour la modélisation de la performance des systèmes multi-états. Ces articles montrent bien les véritables intérêts de l'utilisation des RB en sûreté de fonctionnement par rapport aux méthodes de modélisation classiques.

Nous avons donc aujourd'hui à notre disposition un certain nombre d'articles de synthèse (Langseth et Portinale 2007 ; Langseth 2008 ; Weber et al. 2012) qui donnent une bonne vue de la maturité de l'application des RB à la sûreté de fonctionnement au sens large. Malheureusement, ce formalisme de modélisation n'est pas encore totalement accepté dans le milieu industriel. L'Institut de la Maîtrise des Risques (IMdR) a soutenu plusieurs projets permettant de promouvoir la modélisation par RB : le projet IMdR P04-7 (Munteanu et al. 2007) auquel nous avons participé, a permis d'évaluer la pertinence de l'approche de modélisation par RB par rapport à 7 problèmes en sûreté de fonctionnement posés par des industriels ; le projet IMdR P09-2 (Guyot et al. 2009) aborde la question de la validation de la modélisation par RB sans véritablement le résoudre.

2.1 Modèles graphiques probabilistes : Réseaux bayésiens

Nous introduisons ici le formalisme des modèles graphiques probabilistes (Pearl 1988). Ces objets mathématiques reposent conjointement sur la théorie des graphes et sur la théorie des probabilités. Ils permettent de représenter un modèle factorisé d'une loi de probabilité jointe de plusieurs variables aléatoires discrètes. La théorie des graphes fournit les outils appropriés pour décrire et exploiter graphiquement les relations de dépendance ou d'indépendance entre les variables. La théorie des probabilités apporte, quant à elle, un formalisme permettant de quantifier les relations de dépendance en associant à chaque variable une loi de probabilité conditionnelle.

Eléments formels

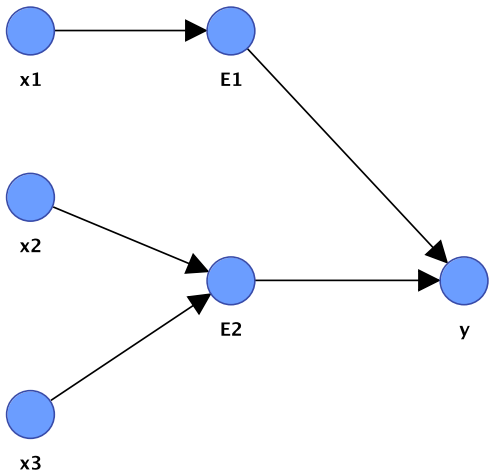


Figure 7 : Modélisation par un RB

Le modèle graphique probabiliste qui nous intéresse est structuré sous la forme d'un graphe orienté sans circuit (DAG : Directed Acyclic Graph). Un DAG est formé de nœuds et d'arcs orientés. Il est commode de classer les nœuds comme nœud parent ou nœud enfant. Un nœud parent est un nœud qui a un ou plusieurs arcs en direction d'autres nœuds. Un nœud

enfant est un nœud connecté à d'autres nœuds par des arcs entrants. Un nœud sans parent est désigné nœud racine et un nœud sans enfant est désigné nœud feuille. Chaque nœud parent x dans un modèle graphique probabiliste est associé à une distribution de probabilité marginale $\mathbb{P}(x)$ et chaque nœud enfant E à une loi de probabilité conditionnelle associée $\mathbb{P}(E|\text{pa}\,(E))$, où pa (E) est l'ensemble de tous les parents de E. Par exemple si nous nous référons à la Figure 7, pa $(E_2) = \{x_2, x_3\}$ et pa $(E_1) = \{x_1\}$.

Toujours selon le modèle graphique probabiliste de la Figure 7, une description complète du modèle, en plus de la structure du graphe repose sur la définition des lois de probabilités a priori : $\mathbb{P}(x_1)$, $\mathbb{P}(x_2)$, $\mathbb{P}(x_3)$ et les lois de probabilités conditionnelles : $\mathbb{P}\,(E_1|x_1)$, $\mathbb{P}(E_2|x_2, x_3)$ et $\mathbb{P}\,(y|E_1, E_2)$. Les lois de probabilités conditionnelles sont définies par une Table de Probabilités Conditionnelles (TPC) exprimant sous la forme d'un tableau ou d'une matrice, les distributions de probabilité d'une variable conditionnellement aux combinaisons des états de ses variables parents. Par exemple la lois de probabilité conditionnelle $\mathbb{P}\,(y|E_1, E_2)$ est définie (Tableau 1), pour les états $\{h_1^y, \dots h_n^y\}$ de y, en fonction des états $\{h_1^{E1}, \dots, h_n^{E1}\}$ de E_1, et des états $\{h_1^{E2}, \dots, h_n^{E2}\}$ de E_2.

Tableau 1

E_1	E_2	$\mathbb{P}(y = h_1^y)$	…	$\mathbb{P}(y = h_n^y)$
h_1^{E1}	h_1^{E2}	$\mathbb{P}\left(y = h_1^y \middle\| E_1 = h_1^{E1}, E_2 = h_1^{E2}\right)$	…	$\mathbb{P}\left(y = h_n^y \middle\| E_1 = h_1^{E1}, E_2 = h_1^{E2}\right)$
	…			
	h_n^{E2}			
…		…		…
h_n^{E1}	h_1^{E2}			
	…			
	h_n^{E2}	$\mathbb{P}\left(y = h_1^y \middle\| E_1 = h_n^{E1}, E_2 = h_n^{E2}\right)$	…	$\mathbb{P}\left(y = h_n^y \middle\| E_1 = h_n^{E1}, E_2 = h_n^{E2}\right)$

Définition : Un modèle graphique probabiliste a pour objet de représenter une loi de probabilité jointe d'un ensemble de variables aléatoires en exploitant les relations de dépendance/indépendance conditionnelles entre ces variables. Un graphe orienté sans circuit permet de représenter ces variables et les relations de dépendance qui les lient. Chaque variable est caractérisée par une loi de probabilité définie conditionnellement à ses variables parents dans le graphe.

Inférence

L'intérêt de la modélisation par RB réside dans sa capacité de calcul. Un RB permet de calculer la distribution marginale de chaque variable en fonction :

- de l'observation de variables connues,
- de vraisemblance sur l'état de certaines variables,
- de la connaissance a priori des lois de probabilités des variables non observées,
- et des lois de probabilités conditionnelles entre les variables.

Les mécanismes internes sont expliqués dans (Jensen, 1996; Pearl, 1988). Il existe plusieurs algorithmes d'inférence permettant les calculs exacts sur des modèles de dimension importante ou encore des inférences approchées pour des modèles de plus grande taille. Ces algorithmes sont utilisés pour intégrer les nouvelles informations i.e. des évidences sous

forme de vraisemblance ou d'observation. Le théorème de Bayes est le cœur de ces mécanismes et permet de mettre à jour l'ensemble des probabilités des variables selon les faits observés et la structure du RB.

Les recherches actuelles portent sur des solutions de plus en plus efficaces pour traiter des modèles de plus en plus complexes et augmenter la quantité de variables prises en compte. Des puissants algorithmes d'inférence exacte exploitent les structures des RB pour résoudre le problème de calcul de la probabilité a posteriori des variables aléatoires (Pearl, 1988; Peot et Shachter, 1991 ; Jensen et al. 1990 ; Shafer, 1996 ; Madsen et Jensen, 1999 ; Faÿ et Jaray, 2000 ; Allen et Darwiche, 2003). L'algorithme d'inférence le plus classique repose sur l'utilisation d'un arbre de jonction, plus d'explications peuvent être trouvées dans (Jensen, 1996, pp. 76). Les algorithmes les plus récents ont pour objectif de limiter les ressources mémoires nécessaires et d'augmenter la vitesse de calcul pour permettre de traiter des problèmes de taille de plus en plus importante (Jaeger, 2002 ; Wuillemin et Torti, 2012).

2.2 Fiabilité et distribution de probabilité jointe

Les RB sont intéressants pour modéliser la sûreté de fonctionnement des systèmes. Ils permettent une modélisation factorisée des relations liant les états des composants aux états du système.

Exemple de système multi-état (voir annexe B pour les détails de modélisation)

Pour mieux cerner l'intérêt des RB appliqués à des problèmes de Sûreté de Fonctionnement, nous proposons d'analyser un système multi-état. La (Figure 8) représente un système à trois vannes $(\mathrm{V1}, \mathrm{V2}, \mathrm{V3})$ utilisé pour réaliser la distribution d'un fluide. Dans ce système les composants sont définis par trois états : un état de fonctionnement normal $\{Ok\}$ et deux états de pannes disjointes ; i.e. un blocage en position fermé $\{Pf\}$ et un blocage en position ouvert $\{Po\}$ (Weber et Jouffe 2003).

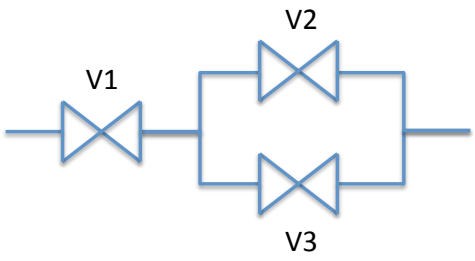


Figure 8. Système à trois vannes.

Distribution jointe

Dans le cas d'un système quelconque, pour définir la distribution jointe, nous avons besoin d'un nombre de probabilités Ω correspondant au produit cartésien de toutes les variables représentant les fonctions et les composants du système (Shafer 1996, page 2). L'avantage de cette représentation est qu'elle permet de représenter de manière exhaustive l'ensemble des situations de fonctionnement et de dysfonctionnement d'un système constitué de

composants multi-états. L'inconvénient majeur est sa taille qui la rend inexploitable pour un analyste dans le cas d'une application industrielle.

Calcul de la fiabilité

La fiabilité du système dépend de l'état des composants. La relation entre l'état du système F et celui des composants est donnée par la fonction de structure. La représentation de la loi de probabilité jointe $\mathbb{P}(\mathrm{F}, \mathrm{V1}, \mathrm{V2}, \mathrm{V3})$ qui décrit l'ensemble des combinaisons d'états des variables du système permet de représenter une fonction de structure quelconque. Dans le cas du système à trois vannes, la fiabilité peut être obtenue à partir de la loi jointe donnée en annexe B. La fiabilité du système est alors donnée par la probabilité $\mathbb{P}(\mathrm{F} = \{Ok\}) = 0{,}345721859$ qui est la somme des probabilités des scénarios de fonctionnement. Il est possible de déduire toutes les probabilités conditionnelles à partir de la distribution de probabilité jointe.

Factorisation

A partir de cette représentation nous pouvons introduire la notion d'indépendance conditionnelle et l'exploiter pour factoriser la loi de probabilité jointe. Les composants V1, V2 et V3 sont indépendants : $\mathbb{P}(\mathrm{V1}, \mathrm{V2}, \mathrm{V3}) = \mathbb{P}(\mathrm{V1}) \cdot \mathbb{P}(\mathrm{V2}) \cdot \mathbb{P}(\mathrm{V3})$. Cependant, l'état de fonctionnement du système $\mathbb{P}(\mathrm{F} = \{Ok\})$ dépend de l'état des composants $\mathrm{V1}, \mathrm{V2}$ et $\mathrm{V3}$. Nous pouvons alors écrire la loi de probabilité jointe sous la forme factorisée suivante :

$$\mathbb{P}(\mathrm{F}, \mathrm{V1}, \mathrm{V2}, \mathrm{V3}) = \mathbb{P}(\mathrm{V1})\ \mathbb{P}(\mathrm{V2})\ \mathbb{P}(\mathrm{V3})\ \mathbb{P}\ (\mathrm{F}|\mathrm{V1}, \mathrm{V2}, \mathrm{V3}) \qquad (1)$$

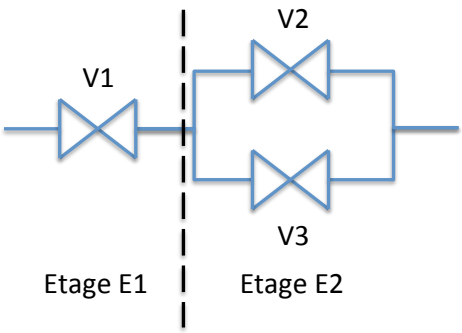


Figure 9. Décomposition du système à trois vannes.

L'équation (1) est une factorisation de la loi de probabilité jointe $\mathbb{P}(\mathrm{F}, \mathrm{V1}, \mathrm{V2}, \mathrm{V3})$. La loi de probabilité conditionnelle déterministe $\mathbb{P}(\mathrm{F}|\mathrm{V1}, \mathrm{V2}, \mathrm{V3})$ reste de dimension importante. Il est intéressant de remarquer que nous pouvons simplifier cette loi en introduisant des variables intermédiaires comme nous le faisons lors de la construction d'un arbre de défaillance. Par exemple, en séparant le système en deux étages comme illustré à la Figure 9. Nous ajoutons les variables E1 et E2 qui permettent de caractériser les étages E1 et E2 du système. La variable E1 caractérise la possibilité de commander le passage du fluide sur l'étage 1, de même pour E2 sur l'étage 2.

Pour conserver toute l'information nécessaire, nous définissons E1 et E2 sur trois états :

- $\{Ok\}$ s'il est possible de commander l'ouverture et la fermeture de l'étage,

- $\{Pf\}$ si l'étage est défaillant et ferme le circuit ne laissant ainsi plus passer de fluide,
- $\{Po\}$ si l'étage est défaillant et reste toujours ouvert laissant passer le fluide en permanence.

L'équation (1) s'écrit alors sous une nouvelle forme factorisée :

$$\mathbb{P}(\mathrm{F},\mathrm{V1},\mathrm{V2},\mathrm{V3}) = \mathbb{P}(\mathrm{V1})\mathbb{P}(\mathrm{V2})\mathbb{P}(\mathrm{V3})\ \mathbb{P}\ (\mathrm{E1}|\mathrm{V1})\ \mathbb{P}(\mathrm{E2}|\mathrm{V2},\mathrm{V3})\ \mathbb{P}(\mathrm{F}|\mathrm{E1},\mathrm{E2}) \qquad (2)$$

Tableau 2

	(*Ok*)	(*Pf*)	(*Po*)
ℙ(V1)	0,31655	0,22782	0,45563
ℙ(V2)	0,19748	0,32095	0,48157
ℙ(V3)	0,14159	0,3678	0,49061

Tableau 3

V2	V3	ℙ(E2=Ok)	ℙ(E2=Pf)	ℙ(E2=Po)
Ok	*Ok*	1	0	0
	Pf	1	0	0
	Po	0	0	1
Pf	*Ok*	1	0	0
	Pf	0	1	0
	Po	0	0	1
Po	*Ok*	0	0	1
	Pf	0	0	1
	Po	0	0	1

Tableau 4

E1	E2	ℙ(F=*Ok*)	ℙ(F=*Hs*)
Ok	*Ok*	1	0
	Pf	0	1
	Po	1	0
Pf	*Ok*	0	1
	Pf	0	1
	Po	0	1
Po	*Ok*	1	0
	Pf	0	1
	Po	0	1

Tableau 5

V1	ℙ(E1=*Ok*)	ℙ(E1=*Pf*)	ℙ(E1=*Po*)
Ok	1	0	0
Pf	0	1	0
Po	0	0	1

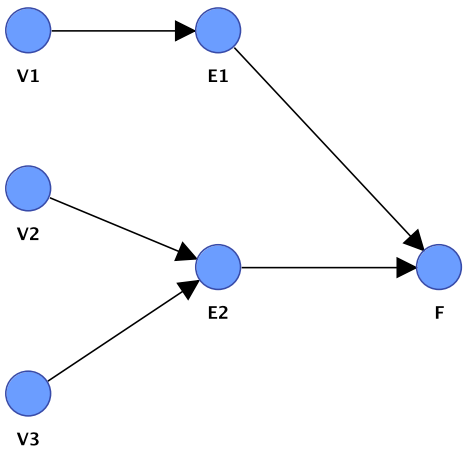


Figure 10. Présentation graphique de la loi jointe factorisée : modélisation par RB

Les distributions de probabilités sur les états des composants (Tableau 2) sont considérées indépendantes et peuvent être définies par rapport à une durée de fonctionnement ou à une date de fin de mission. Elles sont estimées à partir de la loi de fiabilité des composants (loi exponentielle, de Weibull, etc.) ou données par un expert.

Les lois de probabilités conditionnelles sont définies par les (Tableau 3, Tableau 4, Tableau 5). Le principe de factorisation permet de simplifier le modèle par un ensemble de lois de probabilités conditionnelles dont la taille est largement inférieure à celle de la loi de

probabilité jointe. Un réseau Bayésien est une représentation graphique de cette loi de probabilité jointe factorisée, ajoutant à la représentation compacte, la formalisation graphique qui facilite son interprétation (Figure 10). Enfin, les algorithmes d'inférence calculent la loi de probabilité marginale de chaque variable par exemple la loi de probabilité de F :

$$\begin{aligned}\mathbb{P}(\mathrm{F} = Ok) &= 0{,}345721859 \\ \mathbb{P}(\mathrm{F} = Hs) &= 0{,}654278141\end{aligned} \tag{3}$$

Nous retrouvons la somme des scénarios de la loi jointe présentée dans l'annexe B pour le calcul de $\mathbb{P}(\mathrm{F} = Ok)$.

2.3 Discussion et conclusion

Les tables qui définissent la loi de probabilité conditionnelle, modélisent la fonction de structure fiabiliste du système. Cette fonction de structure est une équation qui décrit la relation entre les états d'un système et les états des composants le constituant. Cette fonction est constante, ce qui implique une loi de probabilité conditionnelle discrète indépendante du temps. La modélisation de loi de probabilité conditionnelle définie par une TPC permet de modéliser des relations quelconques entre les états des composants et les états du système. De cette manière, la fonction de structure décrit l'ensemble des scénarios de fonctionnement et de dysfonctionnement du système. La TPC contient donc toute la connaissance nécessaire à l'analyste.

Dans les cas plus classiques où l'hypothèse d'états binaires est faite, i.e. les composants et le système ont deux états $\{Ok, Hs\}$, la fonction de structure est une relation binaire traduite par la TPC. Il y a alors une correspondance exacte du modèle par RB avec un diagramme de fiabilité ou un arbre de défaillance. Dans la représentation que nous avons choisie, la fonction de structure n'est pas binaire car les composants ainsi que le système peuvent avoir plusieurs états de fonctionnements ou de dysfonctionnements. Il n'y a pas de correspondance avec une représentation par un diagramme de fiabilité ou un arbre de défaillance.

Dans l'exemple proposé comme dans tous les cas des fonctions de structures binaires, il n'y a pas d'incertitude sur la combinaison des composants conduisant au fonctionnement ou au dysfonctionnement du système. Les probabilités de $\mathbb{P}(\mathrm{F}|\mathrm{V1}, \mathrm{V2}, \mathrm{V3})$ sont soit égales à zéro soit égales à un. Il s'agit d'une loi de probabilité conditionnelle déterministe. Cela n'est pas une obligation dans un modèle RB. Un modèle non déterministe $\mathbb{P}(\mathrm{F}|\ \mathrm{V1}, \mathrm{V2}, \mathrm{V3}) \in [0,1]$ pourrait être formalisé. Cette représentation par une loi de probabilité conditionnelle non déterministe permet de modéliser des situations où il existe une incertitude sur la conséquence d'une combinaison d'états des 'composants' (par exemple intégrant des opérateurs humains ou un environnement de fonctionnement incertain).

Nous retrouvons ici les avantages majeurs des RB. Il faut noter qu'il n'y a pas de raison de passer par la loi jointe et qu'une construction graduelle du RB permet de formaliser directement la représentation factorisée, ce qui est l'objet de mes travaux de recherche.

3 Réseaux bayésiens : formalisme de modélisation de la fonction de structure des systèmes complexes multi-états

L'une des caractéristiques des modèles graphiques probabilistes qui séduit de nombreux analystes est que le modèle peut être construit directement à partir des connaissances développées par l'expérience sans besoin d'une connaissance détaillée des techniques de calculs utilisées. Cependant, cet avantage peut aussi être source de doute sur la validité des résultats obtenus. Formellement, les résultats sont corrects et la question de la validité ne doit porter que sur le modèle élaboré par l'analyste et/ou sur les données d'entrées, notamment si elles proviennent de l'expertise. Il est donc important de suivre une démarche structurée de modélisation pour élaborer un modèle reflétant la réalité.

En sûreté de fonctionnement, il y a souvent peu d'information disponible, particulièrement dans les domaines de fiabilité, de l'analyse de risque et de la maintenance. Il est donc souvent impossible d'obtenir les paramètres décrivant la loi jointe. C'est pourquoi, les outils de modélisation font principalement appel au jugement d'experts pour construire des modèles structurés (Celeux et al., 2006). La modélisation par RB reste dans cette logique.

C'est une solution de modélisation puissante pour les systèmes complexes car un RB permet de fusionner des connaissances de natures diverses au sein d'un même modèle : les données de retour d'expérience, le jugement d'experts (qui s'exprime par des règles logiques, des équations ou des probabilités subjectives), le comportement du système étudié (l'analyse fonctionnelle et dysfonctionnelle) et des observations. De plus, un RB formalise des relations de cause à effet entre les variables pour modéliser leurs dépendances. Par exemple, un RB peut modéliser l'effet d'actions humaines de maintenance et l'impact des barrières de défense sur l'analyse de risques de systèmes comme cela est proposé dans la thèse (Léger, 2009).

Comme nous l'avons montré, les Réseaux Bayésiens sont tout particulièrement adaptés à la modélisation de la fonction de structure des systèmes. Cette modélisation repose sur des connaissances statistiques qui utilisent une combinaison de données et des connaissances sur les relations causales qualitatives décrivant des dépendances conditionnelles entre les variables. La fonction de structure est utilisée en sûreté de fonctionnement pour la modélisation de la propagation des événements de défaillance, de dégradation et d'altération du fonctionnement des systèmes (Villemeur, 1988, p. 158 ; Cocozza-Thivent, 1997, p. 231 ; Corazza, 1975, p. 114 ; Gertsbakh, 2000, p. 1).

Il est important de remarquer qu'il existe plusieurs structures de réseaux Bayésiens pour un même problème, exactement comme il existe plusieurs représentations par arbre de défaillance ou par diagramme de fiabilité équivalent à une fonction de structure. La structure des modèles sera différente selon la technique de construction du modèle, mais les estimations seront identiques si la même information est encodée, c'est à dire la même loi jointe.

La structure du modèle graphique probabiliste peut être construite à partir des coupes minimales ou des chemins de succès. Nous défendons, dans nos recherches, qu'une analyse fonctionnelle complétée d'une analyse dysfonctionnelle du système (SADT et AMDEC ou HAZOP) permet de formaliser un modèle graphique probabiliste tel que nous l'avons expliqué dans l'article Weber et Jouffe (2006), dans le projet SKOOB et la thèse de Gabriela Medina Oliva (2011). Cette méthode à l'avantage d'éviter la fastidieuse tâche d'énumération des coupes minimales ou des chemins de succès. Nous présentons dans la partie suivante les représentations et l'équivalence des RB obtenus quelle que soit la méthode de construction du modèle utilisée.

3.1 Modélisation par RB dans le cas booléen

Dans l'annexe C, nous expliquons en détail les méthodes de construction d'un modèle graphique probabiliste dans le cas booléen, ce qui permet de comparer les résultats avec les techniques de calcul par coupes minimales, par chemins de succès ou par arbre de défaillances. Pour alléger le document nous ne présentons ici que les résultats de la modélisation et de l'inférence. Ceci nous permet d'introduire la modélisation par nœud papillon appliqué en maîtrise des risques. Ce modèle est l'un des éléments clé de la modélisation exploitée dans les travaux de recherche que nous avons menés en collaboration avec EDF durant les thèses (Léger, 2009 et Fallet, 2012).

Système binaire étudié

Nous proposons d'étudier le système de distribution de fluide dont le diagramme de fiabilité est donné Figure 11. En considérant que les composants n'ont que 2 états : $x_i = 0$ si la vanne i fonctionne et laisse passer le fluide et $x_i = 1$ si la vanne i ne laisse pas passer le fluide. Les distributions de probabilités des x_i sont données (Tableau 6).

Construction du Réseau Bayésien à partir des liens minimaux ou des coupes minimales

Il existe pour le système donné par la Figure 11, deux liens minimaux (scénarios de fonctionnement du système) et deux coupes minimales (scénarios de dysfonctionnement du système) :

$$\begin{aligned} L_1 &= \{x_1, x_2\} \\ L_2 &= \{x_1, x_3\} \end{aligned} \qquad (4)$$

$$C_1 = \{x_1\}$$
$$C_2 = \{x_2, x_3\} \quad (5)$$

Tableau 6

	$\mathbb{P}(x_i = 0)$	$\mathbb{P}(x_i = 1)$
x_1	0,77218	0,22782
x_2	0,67905	0,32095
x_3	0,6322	0,3678

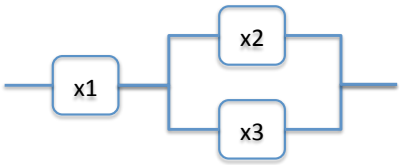


Figure 11 : Diagramme de fiabilité du système de distribution de fluide

Tableau 7

x_1	x_2	$\mathbb{P}(L_1$=0)	$\mathbb{P}(L_1$=1)
0	0	1	0
	1	0	1
1	0	0	1
	1	0	1

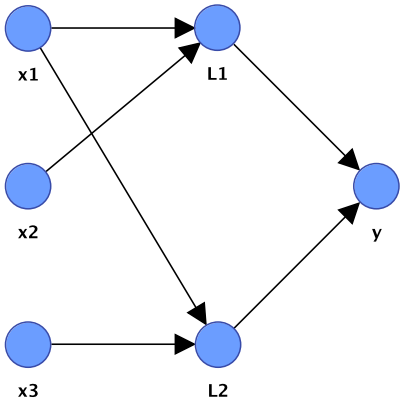


Figure 12 : RB modélisant les relations de dépendances entre les liens minimaux du système.

Tableau 8

x_1	x_3	$\mathbb{P}(L_2$=0)	$\mathbb{P}(L_2$=1)
0	0	1	0
	1	0	1
1	0	0	1
	1	0	1

Tableau 9

L_1	L_2	$\mathbb{P}(y$=0)	$\mathbb{P}(y$=1)
0	0	1	0
	1	1	0
1	0	1	0
	1	0	1

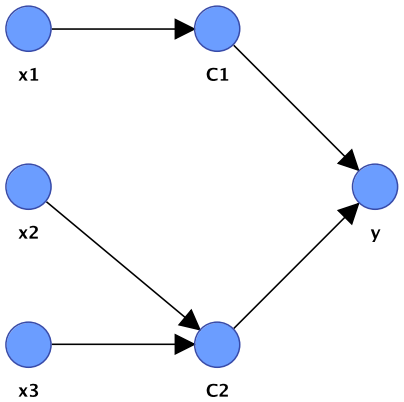


Figure 13 : RB modélisant les relations de dépendances entre les coupes minimales et le système.

Tableau 10

y	
0	0,681027695
1	0,318972305

Pour définir un RB, nous définissons une variable pour chaque lien minimal, les parents des liens sont les variables dont ils dépendent : pa $(L_1) = \{x_1, x_2\}$ et pa $(L_2) = \{x_1, x_3\}$. Le lien existe $(L_j = 0)$ si les composants le constituant sont dans un état de fonctionnement $(x_i = 0)$. Nous pouvons traduire cela par la TPC (Tableau 7 et Tableau 8). S'il existe l'occurrence d'au moins un lien minimal alors le système est dans un état de fonctionnement. Ceci est défini par la TPC (Tableau 9). La structure du RB est donnée par la Figure 12. Le même raisonnement est fait à partir des coupes minimales. La structure du modèle par RB est présentée (Figure 13), les TPC sont présentées dans l'annexe C. Par

inférence, à partir des distributions associées aux composants x_i (Tableau 6), la distribution marginale sur la variable y est donnée par le tableau (Tableau 10). Dans les deux cas (modélisation par les liens minimaux ou par les coupes minimales), les TPC ont des formes standard OU et ET. Enfin, il est à noter que si l'analyste encode des liens (resp. coupes) plutôt que liens **minimaux** (resp. coupes **minimales**) le résultat n'est pas affecté, la structure du modèle est simplement plus lourde.

Construction du Réseau Bayésien par une approche descendante

Dans le cas de grands systèmes l'énumération de tous les scénarios de fonctionnement ou de dysfonctionnement est fastidieuse. Pour résoudre ce problème la construction de modèles par Arbre de Défaillance est fondée sur le principe d'analyse descendante d'un évènement sommet vers les évènements élémentaires (racines ou feuilles).

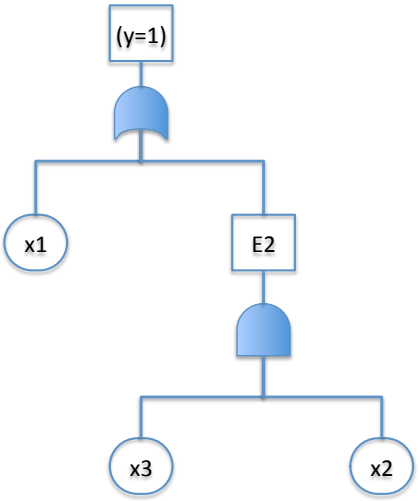


Figure 14 : Arbre de défaillance du système de distribution de fluide.

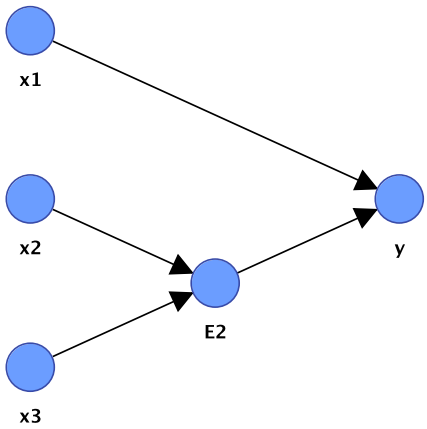


Figure 15 : RB modélisant les relations de dépendances des évènements de l'arbre de défaillance.

Tableau 11

x_2	x_3	$\mathbb{P}(E_2 = 0)$	$\mathbb{P}(E_2 = 1)$
0	0	1	0
	1	1	0
1	0	1	0
	1	0	1

Tableau 12

x_1	E_2	$\mathbb{P}(y = 0)$	$\mathbb{P}(y = 1)$
0	0	1	0
	1	0	1
1	0	0	1
	1	0	1

La structure du RB peut être déduite à partir d'une démarche identique, ou directement à partir d'un arbre de défaillance existant. Pour construire un RB équivalent à l'arbre de défaillance présenté Figure 14, une variable aléatoire discrète est définie pour chaque événement. Les TPC permettant de définir les évènements intermédiaires (E_j) sont construites en fonction des portes logiques (ET, OU, k/n, etc.) de l'arbre de défaillances. Par exemple, pour une porte ET, $(E_2 = x_2 \wedge x_3)$ si les deux composants sont défaillants $(x_i = 1)$ alors l'événement E_2 est occurrent c'est à dire $E_2 = 1$ (Tableau 11). Une porte OU est modélisée (Tableau 12). Par inférence, le RB calcule à partir des distributions associées aux

composants x_i (Tableau 6), la distribution sur la variable y est toujours identique à celle présentée dans le (Tableau 10).

Remarque : Toutes les portes logiques peuvent être représentées dans un RB (OU, ET, k/n, OU exclusif…). Pour cela, il suffit simplement de retranscrire la table de vérité de la fonction logique dans la TPC (Simon et al. 2007 ; Simon et al. 2008). La prise en compte de contraintes topologiques comme dans les systèmes k/n consécutifs linéaires ou circulaires non modélisables par arbres de défaillances est également modélisée facilement par RB (Weber et al. 2010 ; Weber et al. 2011).

Construction de Réseau Bayésien équivalent à un nœud papillon

Il est possible de définir un RB équivalent aux arbres d'événements utilisés en maîtrise des risques pour la propagation des impacts d'un événement initial. Le RB offre une très bonne solution pour représenter dans un seul modèle un nœud papillon comme illustré (Figure 16). Nous avons exploité cette technique de modélisation dans la thèse (Léger 2009), elle est également reprise dans l'article (Khakzada et al. 2013). Les variables Ip_i modélisent les impacts que l'événement $(y = 1)$ a sur le système, sur l'environnement du système, sur les opérateurs, etc.

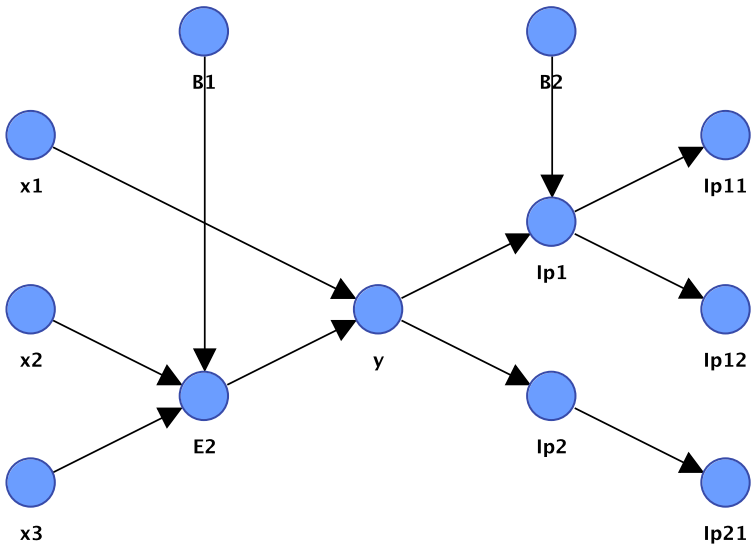


Figure 16 : Modèle RB d'un Nœud papillon et ses barrières

Des barrières de défense (prévention ou protection) peuvent être ajoutées au modèle du nœud papillon pour évaluer leur impact sur la propagation des événements (Figure 16). Une barrière agit comme un inhibiteur, c'est à dire que si elle est mise en place, elle empêche la propagation de la défaillance ou réduit ou mitige ses impacts. Un exemple est donné en fin d'annexe C. Les variables B_i représentant l'efficacité des barrières. La modélisation de l'efficacité des barrières peut être formalisée sous la forme d'un graphe fusionnant les facteurs de perte d'efficacité à la manière d'un arbre de défaillance perpendiculaire au nœud papillon. Les travaux de thèses (Léger, 2009 ; Fallet, 2012) ont porté sur l'estimation de cette efficacité, à partir d'avis d'experts, en fonction de facteurs humains, organisationnels et environnementaux.

Applications

Différentes approches ont été développées ces dernières années afin de proposer une vision globale des risques techniques, humains, organisationnels et environnementaux. Parmi elles, nous avons participé au développement, en collaboration avec EDF et l'INERIS (L'Institut National de l'Environnement Industriel et des Risques), d'une méthode d'AidR (Analyse intégrée des Risques). Cette méthode propose un modèle unifié à la fois multidisciplinaire et générique reposant sur un nœud papillon qui sert à intégrer l'ensemble des connaissances propagées à travers les barrières vers les conséquences de la situation accidentelle.

Les travaux de la thèse (Léger 2009) ont permis l'évaluation quantitative des risques relatifs à l'exploitation d'un système industriel ainsi qu'à l'évaluation de l'impact des parades techniques, humaines et d'organisations (Léger et al. 2008). La contribution repose sur la proposition d'une démarche structurée de modélisation unifiée du système sous différents points de vue. Nous avons proposé une structuration du modèle en niveaux organisation / action / nœud papillon (Léger et al. 2008a, 2008b), (Figure 17). Le modèle est utilisé pour estimer la probabilité d'occurrence des scénarios de risque et évaluer l'impact de barrières sur les performances globales du système.

Nous avons travaillé sur la formalisation de ce modèle de manière générique transposable sur différentes situations. La structuration du modèle en permet une meilleure maîtrise et exploitation, mais elle est aussi une garantie de sa cohérence et de sa pertinence. Notre proposition a été confortée par une application sur une installation chimique (Léger et al. 2009) (avec 80 variables), ainsi que sur un système critique en production d'énergie électrique de EDF (Duval et al. 2012) présenté par la Figure 18 (avec 110 variables).

L'approche proposée dans la thèse (Léger 2009) a été étendue dans la thèse (Fallet 2012) qui propose une amélioration en termes de modélisation et de traitement des connaissances issues principalement du retour d'expérience statistique et des avis d'experts. La structuration du modèle est conservée, mais la théorie de l'évidence est exploitée pour modéliser et traiter des connaissances et leur incertain (Fallet et al. 2010). En s'appuyant sur cette théorie la thèse (Fallet 2012), propose trois contributions pour la modélisation et le traitement de l'incertain dans un modèle AiDR. La première concerne la formalisation de « *l'élicitassion*[2] des risques par avis d'experts » en proposant différentes solutions de collecte flexible et plus adaptée aux différentes connaissances des experts (Fallet et al. 2011). La seconde porte sur la structuration d'un modèle évidentiel des risques permettant de représenter le plus fidèlement possible les différentes expressions des connaissances et d'estimer les risques et leurs incertitudes (Fallet et al. 2012). Enfin, la dernière contribution porte sur l'aide à la décision en univers incertain par une méthode de raffinement du modèle en présence d'incertain (identification des contributeurs à l'incertain) et dans le cas d'incertain non réductible permettant d'évaluer la prise de risque (Fallet 2012).

L'application de ces contributions sur un cas réel de l'industriel EDF permet une comparaison entre le modèle RB (Léger 2009) et le modèle évidentiel (Fallet 2012). Cette comparaison

[2] En Gestion des Connaissances, « éliciter » est l'action d'aider un expert à formaliser ses connaissances pour permettre de les sauvegarder et/ou les partager. C'est laction d'inviter l'expert à rendre ses connaissances tacites en connaissances aussi explicites que possible.

met en évidence les apports au regard d'approches plus conventionnelles du modèle évidentiel permettant de propager des intervalles de probabilités (Fallet-Fidry et al. 2012a, 2012b).

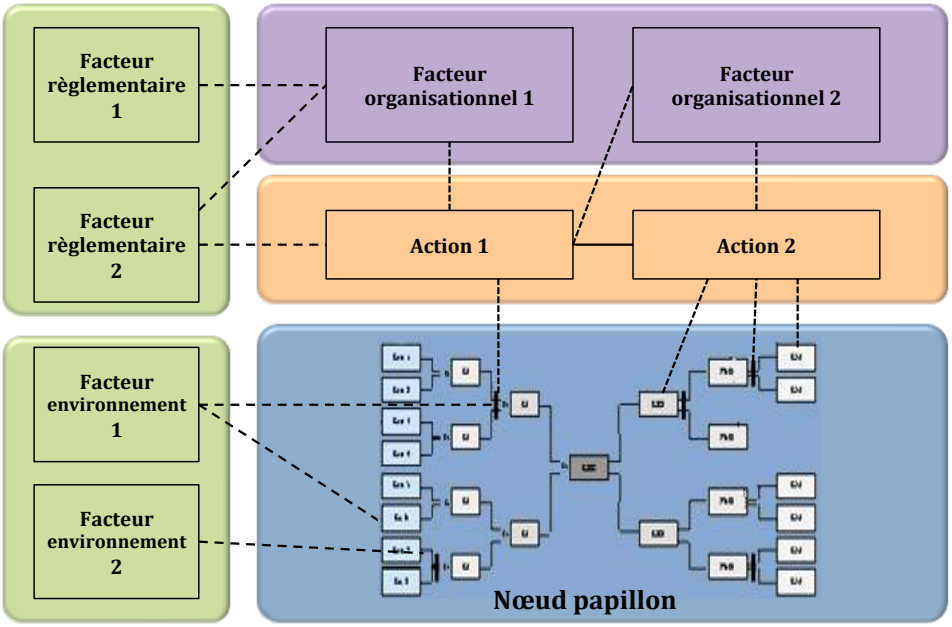


Figure 17 : Structuration du modèle en niveaux organisation / action / nœud papillon

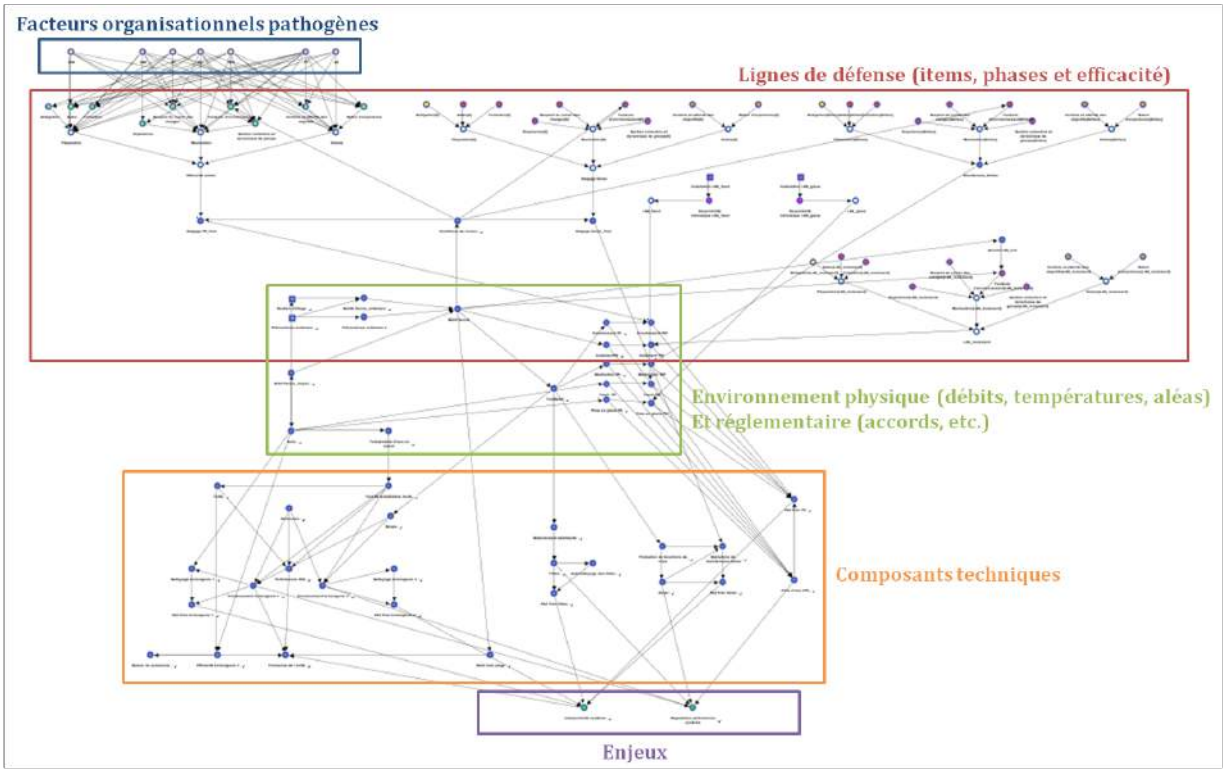


Figure 18 : Modèle RB d'analyse de risque d'un système de production d'énergie

3.2 Modélisation par RB dans le cas multi-état.

Dans le cas de systèmes multi-états, les techniques de modélisation en sûreté de fonctionnement proposées dans la littérature sont difficiles à mettre en œuvre (Lisnianski et Levitin 2003). Nous allons montrer dans cette partie que, en appliquant la démarche de construction de modèle présentée en binaire, nous pouvons formaliser des modèles multi-états sous la forme de réseaux bayésiens. Les explications détaillées sont données dans l'annexe D. Nous présenterons ensuite notre démarche de construction sur le principe d'analyse descendante telle que celle formalisée pour la construction des arbres de défaillances.

Formalisation des variables

Dans le cas d'un système multi-état, nous définissons les variables x_i qui représentent les composants (Shubin et al. 2010) :

$x_i = 0$ si le composant i est en fonctionnement normal (bon fonctionnement),
$x_i = \{1 \dots (l_i - 1)\}$ si le composant i est dans un état de fonctionnement dégradé, (6)
$x_i = \{l_i \dots n_i\}$ si le composant i est dans un état de dysfonctionnement,

avec l_i le premier état de panne du composant, c'est à dire que le composant ne satisfait plus les objectifs de fonctionnement attendu. Les états $\{1 \dots (l_i - 1)\}$ sont des états de fonctionnement dégradés c'est à dire que le composant n'est pas en état de bon fonctionnement, il est altéré ou dégradé, mais il n'empêche pas l'atteinte des objectifs de fonctionnement du système. Les états $\{l_i \dots n_i\}$ sont des états de panne du composant qui peuvent avoir des conséquences différentes sur le système. Ces états peuvent être mis en relation avec les modes de défaillances observés sur le système.
L'état du système est lui aussi défini par une variable multi-état en relation avec les scénarios de fonctionnement et les scénarios de dysfonctionnement du système. Le système est modélisé par une variable y qui prend les valeurs suivantes :

$y = 0$ correspond au fonctionnement normal (bon fonctionnement),
$y = \{1 \dots (l - 1)\}$ correspond à un état de fonctionnement dégradé, (7)
$y = \{l \dots n\}$ correspond à des états de dysfonctionnement du système.

Il est alors difficile, voir impossible, de représenter un tel système par un arbre de défaillance ou un diagramme de fiabilité. Cependant, les notions de coupes minimales et de chemins de succès permettent de définir totalement les relations entre les états du système et les états des composants. Il s'agit donc de l'élaboration d'une fonction de structure ϕ multi-état (non binaire) en considérant les états 0 à n du système. La fonction ϕ permet de relier les états des composants aux états du système telle que $y = \phi(x)$, où $x = (x_1, x_2, \dots, x_r)$.

Construction du modèle Réseau Bayésien

La fonction de structure multi-état du système est facilement modélisée par un RB. Les variables du RB modélisent les états des composants et du système. Il reste à structurer le modèle pour encoder les scénarios de fonctionnement ou de dysfonctionnement.

Une première solution consiste à faire la liste des liens minimaux ou des coupes minimales. En appliquant la même démarche que dans le cas binaire, nous définissons un RB qui représente les dépendances conditionnelles reliant le fonctionnement ou le dysfonctionnement du système aux coupes ou aux liens minimaux. Pour le système (Figure 8), il existe 7 scénarios pour lesquels le système est dans un état de fonctionnement ($y = 0$). Les liens minimaux du système sont définis à partir des combinaisons d'état des composants suivantes : 0 correspond à $\{Ok\}$, 1 correspond à $\{Pf\}$, 2 correspond à $\{Po\}$.

$$\begin{aligned} L_1 &= \{x_1 = 0, x_2 = 0\} \\ L_2 &= \{x_1 = 0, x_3 = 0\} \\ L_3 &= \{x_1 = 0, x_2 = 2\} \\ L_4 &= \{x_1 = 0, x_3 = 2\} \\ L_5 &= \{x_1 = 2, x_2 = 0, x_3 = 0\} \\ L_6 &= \{x_1 = 2, x_2 = 1, x_3 = 0\} \\ L_7 &= \{x_1 = 2, x_2 = 0, x_3 = 1\} \end{aligned} \tag{8}$$

Le lien existe ou fonctionne $(L_j = 0)$ si les composants le constituant sont dans l'état spécifié dans le lien L_j. S'il existe au moins un lien minimal tel que $(L_j = 0)$ alors le système fonctionne $(y = 0)$. En reliant y à chaque lien minimal et en liant chaque lien minimal L_j aux variables x_i apparaissant dans le lien nous obtenons la structure du RB de la (Figure 19).

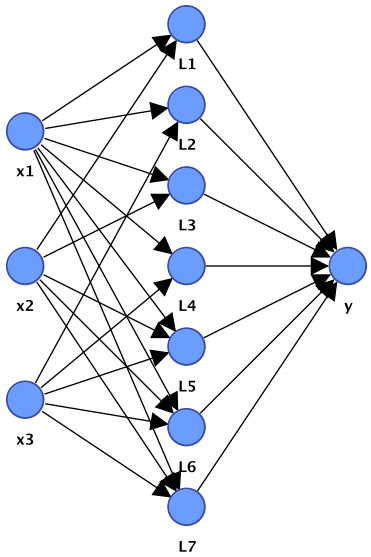


Figure 19 : RB structuré par les liens minimaux pour un système multi-état.

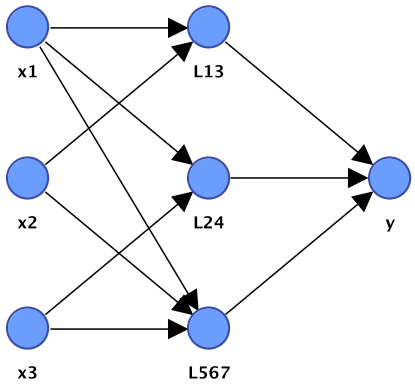


Figure 20 : RB compact, structuré par les liens minimaux pour un système multi-état.

Cette approche permet de générer le RB automatiquement mais conduit rapidement à un modèle peu compact et donc peu lisible. Il est alors judicieux de compacter le réseau en fusionnant les nœuds représentant des liens minimaux connectés aux mêmes variables tels que $\{L_1, L_3\}$, $\{L_2, L_4\}$ et $\{L_5, L_6, L_7\}$ en créant des variables représentant des liens minimaux complexes et en utilisant pleinement les capacités des TPC basées sur une logique de combinaisons multi-états. Pour le cas $\{L_1, L_3\}$ nous définissons : $L_{13} = \{L_1 \cup L_3\}$, $L_{13} = 0$ pour les deux scénarios : $L_1 = \{x_1 = 0, x_2 = 0\}$ et $L_3 = \{x_1 = 0, x_2 = 2\}$; dans tous les autres cas $L_{13} = 1$ (Tableau 13). Pour L_{24} la TPC est définie de la même manière et est identique (Tableau 14). Enfin pour L_{567} la variable est dans l'état 0 pour les trois scénarios : $L_5 = \{x_1 = 2, x_2 = 0, x_3 = 0\}$, $L_6 = \{x_1 = 2, x_2 = 1, x_3 = 0\}$, $L_7 = \{x_1 = 2, x_2 = 0, x_3 = 1\}$ (Tableau 15). La structure plus compacte du RB est présentée à la (Figure 20). Par inférence dans le RB, nous retrouvons pour y les valeurs de la loi de probabilité données à l'éq. (3) ainsi que les probabilités de fonctionnements des liens L_i (Tableau 16).

Tableau 13

x_1	x_2	$\mathbb{P}(L_{13} = 0)$	$\mathbb{P}(L_{13} = 1)$
0	0	**1**	**0**
	1	0	1
	2	**1**	**0**
1	0	0	1
	1	0	1
	2	0	1
2	0	0	1
	1	0	1
	2	0	1

Tableau 14

x_1	x_3	$\mathbb{P}(L_{24} = 0)$	$\mathbb{P}(L_{24} = 1)$
0	0	**1**	**0**
	1	0	1
	2	**1**	**0**
1	0	0	1
	1	0	1
	2	0	1
2	0	0	1
	1	0	1
	2	0	1

Tableau 15

x_1	x_2	x_3	$\mathbb{P}(L_{567} = 0)$	$\mathbb{P}(L_{567} = 1)$
0	0	0	0	1
		1	0	1
		2	0	1
	1	0	0	1
		1	0	1
		2	0	1
	2	0	0	1
		1	0	1
		2	0	1
1	0	0	0	1
		1	0	1
		2	0	1
	1	0	0	1
		1	0	1
		2	0	1
	2	0	0	1
		1	0	1
		2	0	1
2	0	0	**1**	**0**
		1	**1**	**0**
		2	0	1
	1	0	**1**	**0**
		1	0	1
		2	0	1
	2	0	0	1
		1	0	1
		2	0	1

Tableau 16

y	
0	0,345721859
1	0,654278141

L_{13}	
0	0,214953278
1	0,785046723

L_{24}	
0	0,20012291
1	0,79987709

L_{567}	
0	0,066539133
1	0,933460867

Construction du modèle Réseau Bayésien par les coupes minimales

La même démarche est appliquée à partir des coupes minimales. Les quatre scénarios de dysfonctionnement sont les suivants :

$$\begin{aligned} C_1 &= \{x_1 = 1\} \\ C_2 &= \{x_2 = 1, x_3 = 1\} \\ C_3 &= \{x_1 = 2, x_2 = 2\} \\ C_4 &= \{x_1 = 2, x_3 = 2\} \end{aligned} \tag{9}$$

Les TPC sont données en annexe D. La structure du modèle est présentée (Figure 21). Cette structure est différente de celle construite à partir des liens minimaux, elle est compacte et exploite la puissance de modélisation des RB. Par inférence dans le RB nous calculons les distributions de y ainsi que des coupes C_1 à C_4 (Tableau 17). Nous retrouvons pour y les valeurs de la loi de probabilité éq. (3).

Tableau 17

y	
0	0,345721859
1	0,654278141

C_1	
0	0,77218
1	0,22782

C_2	
0	0,88195459
1	0,11804541

C_3	
0	0,780582261
1	0,219417739

C_4	
0	0,776463366
1	0,223536634

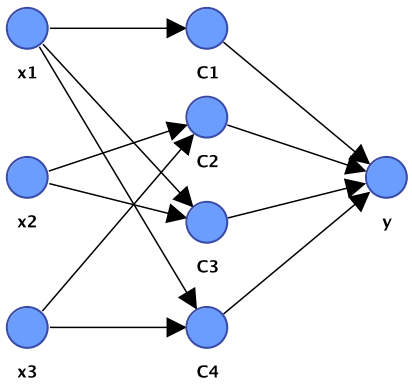


Figure 21 : RB structuré par les coupes minimales pour un système multi-état.

Comme nous l'avons vu, à partir des liens ou des coupes minimales, il est toujours possible de construire un RB que cela soit pour des systèmes simples, complexes, binaires ou multi-états. Les modèles des figures (Figure 19, Figure 20, Figure 21) sont strictement équivalents car ils modélisent la même distribution jointe. Une construction automatique est envisageable. Cependant, les modèles ainsi obtenus sont de grande dimension et n'ont pas une structure très explicite. Cette structuration en trois couches : composants ; coupes ou liens minimaux ; missions du système, n'est pas très lisible dans le cas de systèmes de grande dimension comme les systèmes industriels.

Construction depuis une analyse fonctionnelle/dysfonctionnelle

Nous avons proposé dans nos travaux de recherche une méthode de construction des modèles graphiques probabilistes multi-états sans passer par cette étape fastidieuse de description de tous les scénarios de fonctionnement ou de dysfonctionnement. Pour cela, nous avons formalisé une méthode de construction du modèle sur la base d'une analyse fonctionnelle couplée avec une analyse dysfonctionnelle dans les articles (Weber et al. 2001 ; Muller et al. 2004 ; Weber et Jouffe 2006 ; Medina-Oliva et al., 2013 et 2015). Cette démarche permet de structurer des modèles RB pour des systèmes multi-états.

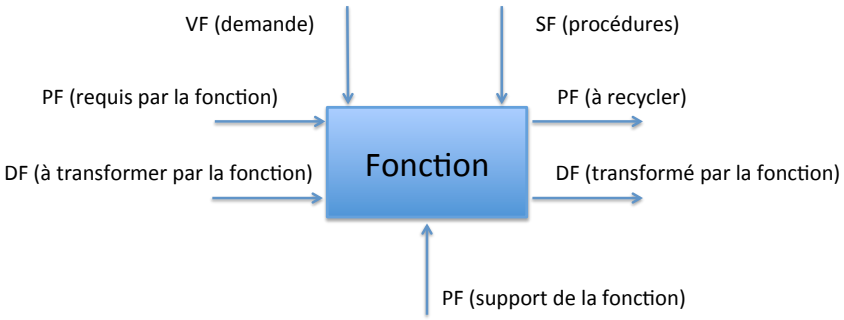


Figure 22 : Définition générique d'une fonction et de ses flux

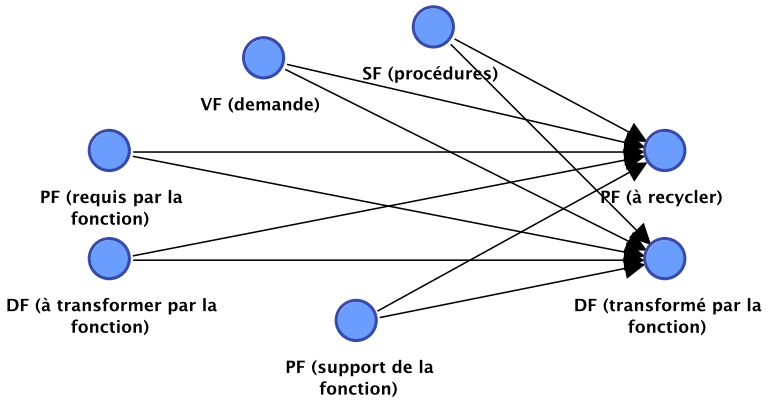


Figure 23 : Motif générique du RB modèle d'une fonction

L'analyse fonctionnelle permet de décomposer le système en faisant apparaître les fonctions du système. Elle permet de spécifier les variables structurant le modèle selon des niveaux d'abstraction décrits par une architecture fonctionnelle. Le système peut être pris au sens large, il ne concerne pas uniquement le système technique, mais peut aussi englober les hommes qui utilisent et maintiennent le système technique (Medina-Oliva, 2011).

Pour qu'une fonction soit correctement réalisée, il est nécessaire de lui fournir un ensemble de «flux» liés à son environnement : condition de fonctionnement, support de fonctionnement, énergie, commandes etc. Plusieurs flux entrants peuvent contribuer à la réalisation d'une fonction. Le motif générique d'une fonction est alors présenté (Figure 22).

Pour chaque fonction définie dans l'analyse fonctionnelle, une brique de modélisation par RB peut être spécifiée. Un nœud du RB est associé à chaque flux entrant ou sortant de la fonction. A partir du motif générique d'une fonction nous définissons le motif générique du RB qui lui est associé (Figure 23).

Les variables peuvent être multi-états et les relations de dépendance entre les variables peuvent être définies par des lois de probabilités conditionnelles quelconques. Les analyses AMDEC et HAZOP permettent de spécifier les états des variables représentant les composants (états de marche, états de marche dégradée, états de panne) ainsi que les flux de sortie des fonctions avec leurs modes de fonctionnement et de dysfonctionnement.

Tableau 18

Flux entrant de la fonction	Variable	Flux sortant de la fonction
PF (V1, V2, V3) ; DF (fluide à transférer) ; VF (commande)	L	DF (L)
PF (V1) ; DF (fluide à transférer) ; VF (commande)	L_1	DF (L1)
DF (L1) ; PF (V2) ; VF (commande)	L_2	DF (L2)
DF (L1) ; PF (V3) ; VF (commande)	L_3	DF (L3)
PF (V1, V2, V3) ; DF (fluide à transférer) ; VF (commande)	I	DF (I)
PF (V1) ; DF (fluide à transférer) ; VF (commande)	I_1	DF (I1)
PF (V2) ; DF (fluide à transférer) ; VF (commande)	I_2	DF (I2)
DF (I2) ; PF (V3) ; VF (commande)	I_3	DF (I3)

Pour illustrer le principe de modélisation nous appliquons cette démarche pour structurer le modèle du système (Figure 8). Une analyse fonctionnelle est donnée en annexe D et rappelée par les (Figure 24, Figure 25, Figure 26 et Figure 27). A partir de la modélisation fonctionnelle, les variables x_1, x_2, x_3 sont associées respectivement aux flux PF (V1), PF (V2), PF (V3), représentant les composants du système. La variable y est associée au flux DF (fluide transféré) et représente la finalité du système. Pour chaque fonction une variable est définie (Tableau 18) représentant son flux de sortie dépendant des flux d'entrée de la fonction.

La structure du RB (Figure 28) est construite simplement en reliant les flux tels que l'analyse fonctionnelle le définit. L'analyse fonctionnelle définit la fonction « Laisser passer 2 » avec le flux de sortie DF (L2) qui est représenté par L_2 dans le RB. Les flux d'entrée de la fonction sont DF (L1), PF (V2) (et VF (commande) non modélisé). Les parents de la variable L_2 sont donc représentés dans le RB par L_1 et x_2. Nous procédons de la même manière pour construire le modèle en connectant toutes les variables représentant les fonctions du système modélisé lors de l'analyse fonctionnelle. Le modèle obtenu est équivalent aux modèles construits à partir des coupes minimales et des chemins de succès, mais cette fois, il repose sur une démarche de construction structurée à partir d'une analyse fonctionnelle du système.

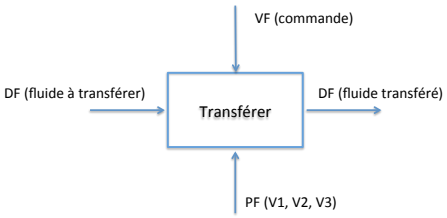


Figure 24 : Modèle fonctionnel du système de transfert de fluide

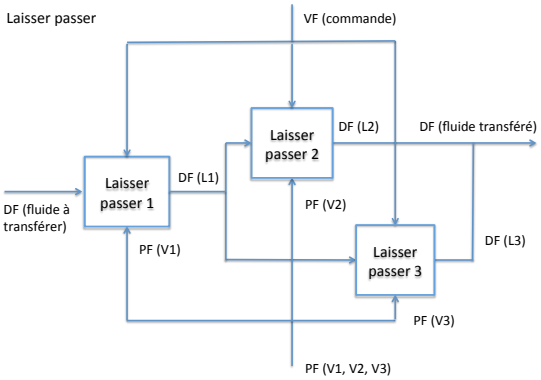


Figure 26 : Modèle fonctionnel du système (fonction Laisser Passer)

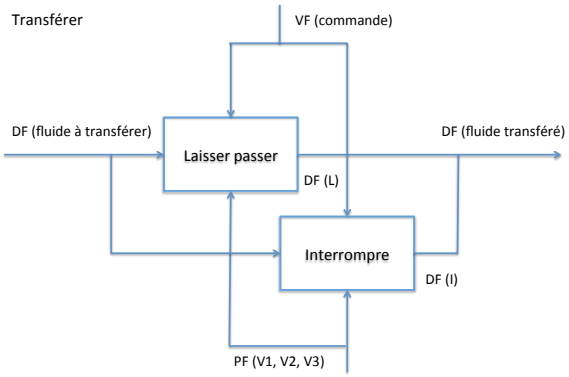


Figure 25 : Modèle fonctionnel du système (fonction Transférer)

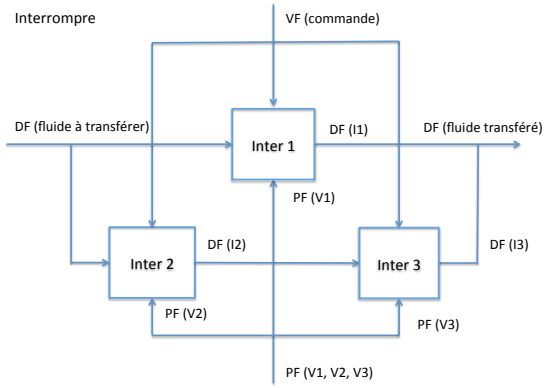


Figure 27 : Modèle fonctionnel du système (fonction Interrompre)

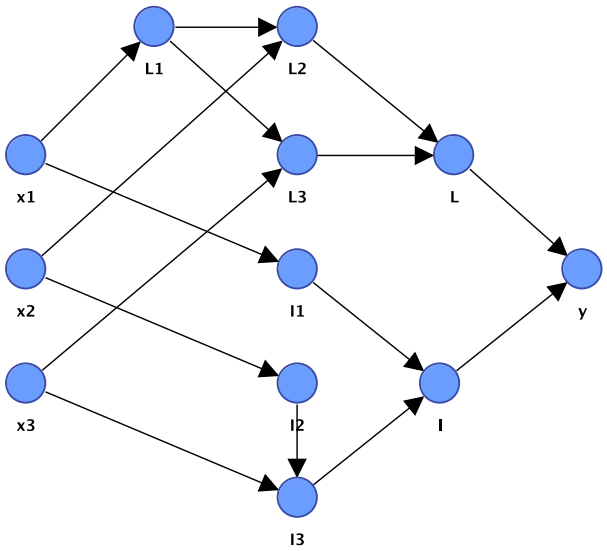


Figure 28 : RB structuré à partir de l'analyse fonctionnelle

Par inférence dans le RB nous calculons la distribution de y. Le résultat est conforme à la distribution éq. (3). Les distributions des variables représentant le découpage fonctionnel du système L et I sont également calculées (Tableau 17), (L_1, L_2, L_3, I_1, I_2 et I_3 sont présentés en annexe D).

Tableau 19

y	
0	0,345721859
1	0,654278141

L	
0	0,681027695
1	0,318972305

I	
0	0,664694164
1	0,335305836

La démarche de construction du RB que nous avons proposée généralise les autres méthodes de modélisation au cas multi-état.

3.3 Applications industrielles

L'intérêt de cette démarche de modélisation prend tout son sens dès qu'il s'agit de modéliser des systèmes de taille importante. Par rapport aux exigences de plus en plus importantes relatives au Maintien en Condition Opérationnelle (MCO) d'un système industriel, le processus de maintenance joue un rôle fondamental pour l'amélioration de la disponibilité, de la productivité. Pour contrôler au mieux ces performances, les responsables de maintenance doivent donc être capables de choisir une stratégie de maintenance et les ressources à mettre en œuvre les plus adaptées aux besoins.

Dans un objectif d'aide à la prise de décision en maintenance, les travaux de thèse (Medina-Oliva 2011) ont permis de formaliser une méthodologie pour l'élaboration d'un modèle permettant par simulation d'évaluer différentes stratégies de maintenance (Medina-Oliva et al. 2011). Le modèle nécessaire est de taille considérable et fusionne de nombreuses vues complémentaires relatives au fonctionnement, au dysfonctionnement, mais aussi en relation avec l'organisation du service maintenance, l'efficacité de sa politique d'action. Il est donc impossible d'imaginer qu'un tel modèle soit formalisé de manière monolithique. La valeur ajoutée de la méthodologie réside dans l'unification, à base de modèles relationnels probabilistes (PRM), des différents types de connaissances nécessaires à la construction de ce modèle d'évaluation (Medina-Oliva et al. 2013, 2015).

Le modèle est construit à partir d'analyses fonctionnelles et dysfonctionnelles. La construction est formalisée sur la base de motifs génériques et modulables représentatifs des variables décisionnelles du système industriel (système principal) et de son système de maintenance (Medina-Oliva et al. 2015). Ces motifs facilitent la construction des modèles par instanciation.

Dans les travaux de thèse (Medina-Oliva 2011, Medina-Oliva et al. 2013) une application est faite pour la modélisation de l'interaction entre maintenance et performance d'un système agroalimentaire, le modèle est présenté par la Figure 29 (avec 700 variables). Lors de l'inférence, le modèle de calcul est construit partiellement pour répondre aux requêtes et n'est jamais représenté en totalité par l'algorithme d'inférence. Cette méthodologie, issue du projet ANR SKOOB (SKOOB, 2011), est testée en partenariat avec l'industriel SOREDAB, sur la maintenance d'un système de production de ferment (Medina-Oliva et al. 2013 et 2015).

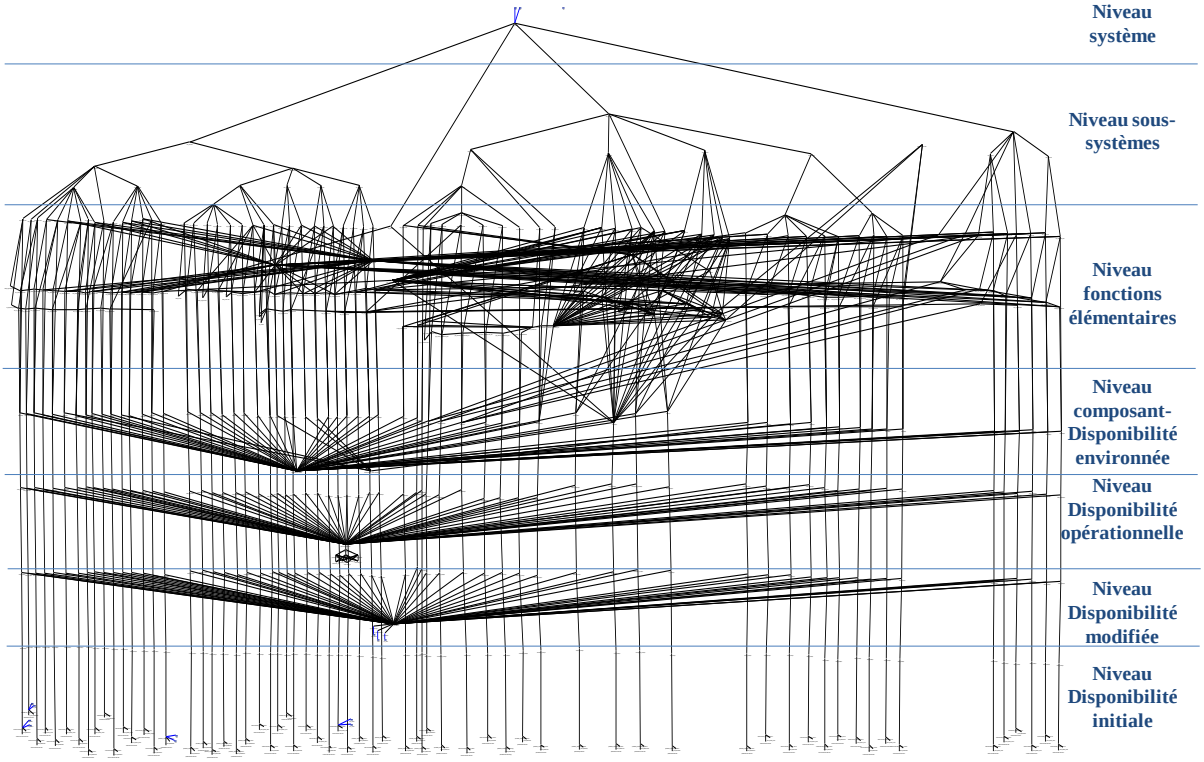


Figure 29 : Modèle RB d'interaction maintenance performance d'un système agroalimentaire

3.4 Conclusion

Nous avons illustré dans cette partie comment les RB peuvent être utilisés pour résoudre les problèmes de la modélisation de systèmes complexes en sûreté de fonctionnement et maîtrise des risques. Ce formalisme de modélisation est très bien adapté à la modélisation de systèmes complexes multi-états dans lesquels les dépendances entre les variables ne sont pas toujours déterministes. Le formalisme de modélisation par RB généralise les formalismes classiques tels que les arbres de défaillances ou diagrammes de fiabilité préconisés par les normes. La modélisation par RB est donc une solution efficace et flexible pour la représentation des systèmes complexes et multi-états.

Il existe plusieurs structures de RB pour un problème donné. La validation du modèle repose principalement sur la méthodologie de construction qui doit être confrontée ensuite à l'expérience, à l'expertise et à des scénarios de test pour valider le fonctionnement du modèle sur des cas connus.

Bien que la modélisation par RB soit très compacte et permette de manipuler plusieurs centaines de variables, nous pouvons avoir à modéliser des milliers de variables dans le cas de grands systèmes industriels. Dans ce cas, les RB arrivent à leurs limites. Quand le nombre de fonctions et de variables devient trop important, c'est à dire que les modèles ne peuvent plus être représentés dans la mémoire des systèmes informatiques qui les manipulent, il est alors nécessaire d'utiliser un formalisme de modélisation plus adapté.

Basé sur nos principes de modélisation nous avons exploité un Modèle Probabiliste Relationnel (PRM : Probabilistic Relational Model) pour la construction de modèle de très grande taille (plus de 700 variables). Les algorithmes d'inférence pour la modélisation PRM sont encore en cours de développement (Sommestad et al. 2010 ; König et al. 2010 ; Gonzales et Wuillemin 2011). A notre connaissance, il n'existe pas encore de plateforme de modélisation PRM à destination des industriels. Les capacités des PRM permettent la capitalisation de connaissance par la création de classes génériques puis celle d'instanciation à un système particulier.

Nous avons donné une illustration de l'utilisation de tels modèles pour l'optimisation de la stratégie de maintenance (Medina-Oliva et al., 2013 et 2015). Dans le cadre du projet ANR SKOOB, un langage (SKOOL) ainsi qu'un moteur d'inférence de modèles PRM ont été appliqués à la modélisation de grands systèmes complexes (SKOOB, 2011). Ce formalisme de modélisation représente, à mon avis, l'avenir des modèles graphiques probabilistes.

Les modèles que nous avons présentés dans cette section sont des modèles statiques, ils ne prennent pas en compte la dimension temporelle. En sûreté de fonctionnement pour pouvoir intégrer l'impact de l'environnement et des conditions d'utilisations du système sur son vieillissement et sa dégradation, il est important de modéliser cette dimension temporelle. Cela permet d'évaluer l'évolution de la probabilité d'occurrence d'évènements en fonction du temps et de prévoir un comportement probabiliste futur. L'objectif est d'anticiper une dégradation du système. Cette dimension temporelle est présentée dans la section suivante.

4 Réseaux Bayésiens Dynamiques : un formalisme de modélisation pour l'intégration de l'environnement et des contraintes d'exploitation dans le calcul de la fiabilité des systèmes

Pour prendre en compte l'incertitude en plus de l'aspect temporel, l'évolution d'un système est représentée comme une variable aléatoire qui prend ses valeurs dans un espace fini d'états correspondant aux états possibles du système. La modélisation à partir de l'espace d'états des processus est utilisée depuis longtemps en sûreté de fonctionnement comme le présente la littérature spécialisée (Corazza 1975 ; Villemeur A. 1988 ; Ansell and Phillips, 1994 ; Cocozza-Thivent 1997 ; Aven and Jensen, 1999 ; Gertsbakh, 2000 ; etc.) ainsi que les normes industrielles (NF EN 61 165, 2006). Les modèles ainsi obtenus permettent d'estimer la valeur de la probabilité de défaillance des systèmes au cours du temps en présence de dépendances entre les composants.

Cette méthode mène à une représentation graphique (Villemeur, 1988, chap. 14 pp. 303 ; Cocozza-Thivent, 1997, chap. 9, pp. 282). La complexité du modèle dépend des suppositions faites pour approcher le processus stochastique réel. Malheureusement, la complexité augmente dramatiquement dès que le nombre de composants augmente. En effet, l'espace

d'états décrivant le système est construit à partir du produit cartésien des états des composants constituant le système.

Des techniques d'agrégations d'états sont proposées (Cocozza-Thivent, 1997, chap. 9, pp. 282). Nous avons utilisé ces techniques pour la modélisation par Chaînes de Markov (CM) appliquée à l'analyse de la fiabilité d'un système de conversion d'énergie électrique (éolienne). Les Chaînes de Markov que nous proposons sont très compactes alors que sans la fusion des états nous aurions eu des modèles avec plusieurs dizaines d'états (Weber et al. 2006, Weber et al. 2008, Pour et al. 2009, Weber et al. 2012b).

La représentation par Arbres de défaillances Dynamiques (AdD) (Dugan et al. 1992, Meshkat et al., 2002) est une des solutions permettant de décrire une CM de grande dimension. La modélisation par AdD repose sur un langage graphique de description de la structure de combinaison des composants (par exemple une structure en redondance passive « Spare Gate »). La CM est générée par compilation du modèle graphique AdD.

De nos jours, il est nécessaire de modéliser des relations de plus en plus complexes pour estimer les comportements dynamiques des systèmes. Les modèles ont pour objectif d'estimer des distributions de probabilité d'état en prenant en compte l'âge des composants, les opérations de maintenance et de conduite et l'évolution de l'environnement du système. La prise en compte de systèmes dans leur globalité et leurs interactions avec l'environnement, conduit à la modélisation d'un nombre de variables important. Cette augmentation du nombre de variables rend une modélisation par CM difficile du fait de l'explosion combinatoire qu'elle provoque sur le nombre d'états du système. Cette explosion combinatoire pose le problème de la lisibilité et de la maintenabilité des modèles (De Souza and Ochoa, 1992). Les AdD sont fondés sur un langage graphique qui atteint alors ses limites, notamment parce qu'il est élaboré à partir d'une représentation binaire, ce qui n'est pas naturellement adapté au cas de systèmes multi-états.

Dans cette situation, la modélisation par RB est intéressante car elle étend les capacités des formalismes de modélisation standard à l'évaluation de la fiabilité des systèmes complexes multi-états. Les RB Dynamiques (RBD) sont connus pour être capables de formaliser des modèles de processus stochastique sous une forme compacte (Murphy, 2002). Les premiers travaux de recherche sur l'application des RBD à la fiabilité et les analyses de disponibilité de systèmes sont proposés par (Welch et Thelen, 2000). Nous avons proposé en 2002 une modélisation de la disponibilité d'un système par RBD (Weber 2002). Puis nous avons montré l'intérêt de l'application à la sûreté de fonctionnement de la capacité de factorisation d'une CM par les RBD dans le cas multi-état (Weber et Jouffe 2003). Cette factorisation permet de réduire la difficulté de manipulation et de construction des modèles et offre la possibilité de modéliser des systèmes plus complexes.

Le but de cette partie est de présenter l'application des RBD en sûreté de fonctionnement, et d'expliquer l'extension qu'ils permettent par rapport à la modélisation par CM. Mais aussi de montrer les limites de ce formalisme, et les besoins d'évolutions des algorithmes d'inférence dans les RBD.

4.1 Formalisation du modèle d'un composant par Réseaux Bayésiens Dynamiques

Un réseau bayésien dynamique permet de prendre en compte la dimension temporelle en décomposant l'espace des variables aléatoires discrètes du réseau bayésien en tranches de temps. Un processus est représenté à l'instant k par une variable $x_i^{(k)}$ avec un nombre fini d'états $\{h_1^x, \dots h_n^x\}$. L'ensemble des variables ayant la même valeur de k forment la tranche de temps k (Hung et al. (1999); Boutillier (1999), pp. 38-45). Un RBD permet de modéliser l'évolution des variables aléatoires discrètes en définissant la dépendance conditionnelle d'une tranche de temps $k+1$ par rapport aux variables définies dans les tranches de temps k précédentes. La définition de la dépendance qui lie les variables des différentes tranches de temps permet de modéliser des processus aléatoires très variés et très complexes. Cette relation temporelle est définie simplement dans un RBD par une table de probabilité conditionnelle (TPC). La Figure 30 est un cas particulier pour lequel une variable $x_i^{(k)}$ n'est définie que conditionnellement à la même variable de la tranche de temps immédiatement antérieure $x_i^{(k-1)}$: c'est la cas markovien.

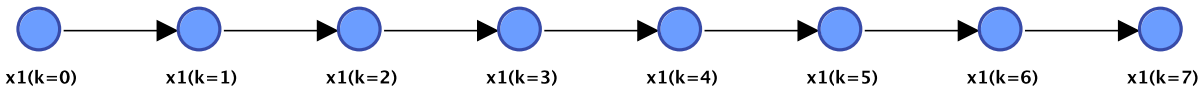


Figure 30 : Modèle RB Dynamique déroulé sur 8 tranches de temps

A partir d'une situation observée à un instant k quelconque ou des conditions initiales par exemple pour $k = 0$, l'algorithme d'inférence du réseau bayésien permet de calculer la distribution de probabilité de toutes les variables pour toutes les tranches de temps. Pour effectuer les calculs, il est nécessaire de mémoriser la totalité des distributions de probabilité des variables. La solution consiste à développer des tranches de temps sur tout l'horizon de calcul souhaité, c'est à dire à dupliquer les variables pour chaque période. Malheureusement le RB augmente proportionnellement à l'horizon de calcul (Kjaerulff 1995), cette solution ne convient pas pour l'analyse de la fiabilité des systèmes car le processus doit être analysé sur un horizon de temps qui conduit à une explosion du nombre de variables à développer dans le modèle que les algorithmes d'inférence actuels peuvent difficilement gérer.

Modèle par RBD d'une Chaîne de Markov

Dans le cas de processus Markoviens, les propriétés du processus sont utilisées pour simplifier l'inférence. Par exemple, pour un processus de Markov invariable dans le temps

(annexe E.1), l'inférence dans le réseau bayésien dynamique peut être réalisé de manière itérative sans expliciter une variable pour chaque tranche de temps. Le modèle RBD est alors formalisé sous une forme compacte en ne faisant apparaitre que deux tranches de temps. Un réseau bayésien à deux tranches de temps 2-TBN (Boyen et Koller 1998) permet de définir tous les paramètres nécessaires à la modélisation d'une Chaîne de Markov. La première tranche comprend les variables à l'instant courant du temps k, la seconde tranche permet le calcul par inférence de la distribution des variables à l'instant $(k+1)$. Une variable $x_i^{(k+1)}$ est définie conditionnellement à ses états dans la tranche de temps immédiatement antérieure $x_i^{(k)}$. La table de probabilité conditionnelle (TPC) de $x_i^{(k+1)}$ est constante quelque soit la valeur de k (Tableau 20). Cette TPC est définie à partir de la matrice de probabilité de transition entre les états de la Chaîne de Markov (donnée dans l'annexe E.1). Avec ce modèle, l'avenir $(k+1)$ est conditionnellement indépendant du passé étant donné le présent (k), la TPC représente bien une Chaîne de Markov (Kjaerulff, 1995).

Tableau 20

$x_i^{(k)}$	$\mathbb{P}\left(x_i^{(k+1)}=0\right)$	…	$\mathbb{P}\left(x_i^{(k+1)}=n_i\right)$
0	$\mathbb{P}\left(x_i^{(k+1)}=0 \middle\| x_i^{(k)}=0\right)$		$\mathbb{P}\left(x_i^{(k+1)}=n_i \middle\| x_i^{(k)}=0\right)$
…			
n_i	$\mathbb{P}\left(x_i^{(k+1)}=0 \middle\| x_i^{(k)}=n_i\right)$		$\mathbb{P}\left(x_i^{(k+1)}=n_i \middle\| x_i^{(k)}=n_i\right)$

Après une première inférence la distribution $\mathbb{P}\left(x_i^{(k+1)}\right)$ est mémorisée et injectée comme distribution *a priori* de $x_i^{(k)}$; une nouvelle inférence permet alors de calculer la distribution pour l'instant suivant. Une inférence exacte calcule la distribution de probabilité de la variable de la tranche de temps $k+1$ à partir de la tranche de temps k. Les distributions de probabilités pour les tranches de temps suivantes $k+2,\ k+3, \ldots$ sont calculées par des inférences successives (Welch et Thelen, 2000). Pour un horizon de h tranches de temps, il faut donc h inférences. Cette méthode de calcul est équivalente à l'équation de Chapman-Kolmogorov.

Modèle par RBD d'un processus à paramètres variables dans le temps

L'extension au cas semi-Markovien est possible en introduisant des TPC indexées par rapport aux temps. Dans notre travail en collaboration avec Bayesia (éditeur du logiciel BayesiaLab), nous avons introduit cette possibilité dans le logiciel Bayesialab. Les RBD permettent de modéliser facilement des processus pour lesquels les paramètres sont variables dans le temps. Les paramètres définis dans la TPC peuvent être indexés par rapport à une variable k qui représente le temps.

Exemple

Pour une vanne, le composant est défini par trois états : un état de fonctionnement normal $\{Ok\}$ et deux états de panne disjointe ; i.e. un blocage en position fermé $\{Pf\}$ et un blocage

en position ouvert $\{Po\}$. Dans le cas de paramètres non constants, nous illustrons ce principe en combinant deux lois de Weibull appliquées à la vanne 1. Les taux de défaillance sont alors considérés variant dans le temps et définis de sorte que les processus des défaillances suivent les lois de Weibull avec les paramètres suivants :

- Pour la défaillance 1, c'est-à-dire un blocage fermé de la vanne, nous utilisons le taux de défaillance défini comme suit :

$$\lambda_{1Pf} = \frac{\beta \cdot k^{(\beta-1)}}{\alpha^{\beta}} \text{ avec } \beta = 3 \text{ et } \alpha = 500$$

- Pour la défaillance 2, c'est-à-dire un blocage ouvert de la vanne, nous utilisons le taux de défaillance défini comme suit :

$$\lambda_{1Po} = \frac{\beta \cdot k^{(\beta-1)}}{\alpha^{\beta}} \text{ avec } \beta = 2{,}5 \text{ et } \alpha = 700$$

Le modèle RBD du composant vanne 1 est présenté par la figure (Figure 31). La distribution de probabilité sur les états de la vanne est calculée sur 1000 heures par 1000 itérations.

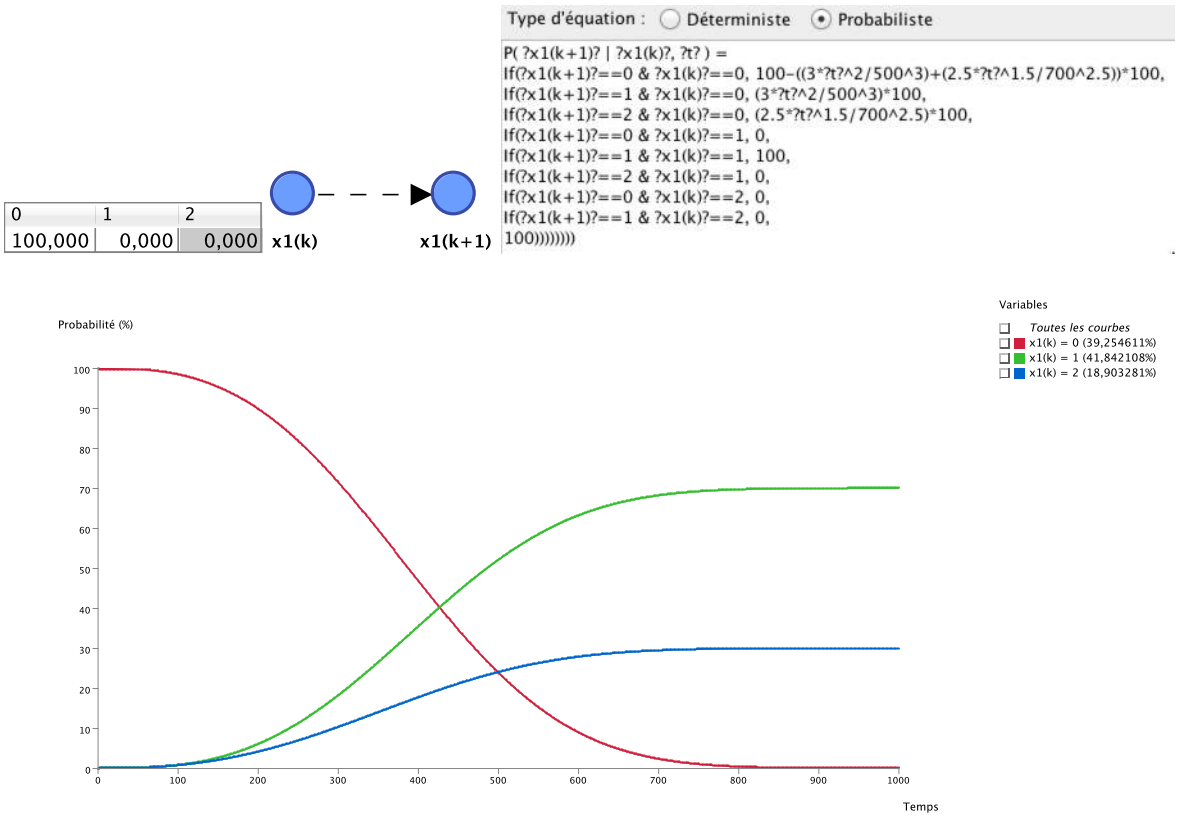


Figure 31 : Modèle RB Dynamique Processus Semi-Markovien

Hypothèse de processus avec contrainte exogène

Comme nous l'avons montré dans l'annexe E.3 et dans nos travaux (Weber et al. 2004), un modèle de Markov caché HMM (Hidden Markov Model : Rabinet, 1989) permet de représenter la dégradation des composants. La modélisation de la dégradation des

composants par HMM a aussi été reprise dans les travaux (Moghaddoss et Zuo, 2012 ; Roblès et al. 2013 ; Le et al. 2014).

Le temps est souvent considéré comme le facteur qui conditionne la fiabilité du composant. Cela peut s'avérer insuffisant (Singpurwalla, 1995), les conditions d'exploitation et l'environnement (par exemple humidité, température) peuvent également altérer la fiabilité d'un composant. Tous ces facteurs qui peuvent impacter la fiabilité d'un composant sont appelés Co-variables ou variables explicatives (Bagdonavicius et Nikulin, 2001). Comme le décrit (Cox, 1955), la fiabilité d'un composant peut être modélisée de manière plus précise en prenant en compte les effets des Co-variables.

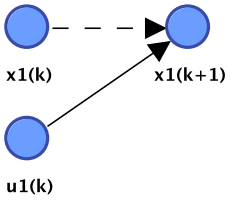
Pour tenir compte des événements exogènes, nous avons proposé (Weber et al. 2004) de définir plusieurs modèles par CM qui représentent chaque situation en fonction du contexte d'exploitation du composant. Un Modèle de Markov Commuté noté MSM pour « Markov Switching Model » peut être introduit pour modéliser ce type de processus stochastique intégrant l'impact d'événements exogènes qui conditionnent le passage d'une CM à une autre. Ces modèles sont également considérés comme des CM conditionnelles où les probabilités de transition sont conditionnelles à une variable exogène.

Les modèles MSM sont non-stationnaires à cause des changements brutaux dans les paramètres du modèle (Bengio 1999 pp 147). Un MSM représente la distribution conditionnelle $\mathbb{P}\left(x_i^{(k)}\middle|u_i^{(k)}\right)$ compte tenu de la séquence d'état de l'entrée $\left[u_i^{(0)}, u_i^{(1)}, \dots u_i^{(k)}\right]$ où $u_i^{(k)}$ représente l'état de la contrainte exogène. La simulation d'un modèle de Markov commuté est basée sur un changement discontinu des paramètres à chaque commutation d'état de la variable exogène. Il est très difficile d'obtenir la solution analytique de ce type de système différentiel hybride.

La modélisation d'un MSM par un RBD est triviale (Weber et al 2004). Une co-variable (permettant de modéliser des contraintes ou les variations de l'environnement du composant) est ajoutée dans le réseau bayésien comme une nouvelle variable aléatoire discrète $u_i^{(k)}$ de la tranche de temps k. La table de probabilité conditionnelle de $x_i^{(k+1)}$ qui régit le comportement du processus est définit conditionnellement à $u_i^{(k)}$ (Figure 32).

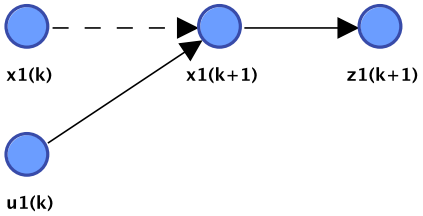
Enfin, nous avons proposé que, si l'état de la variable exogène $u_i^{(k)}$ n'est pas connu, mais une séquence de distribution de probabilité permet de décrire ses états, le processus stochastique, permettant de modéliser un composant et son environnement, est formalisé sous la forme d'un processus de Markov caché conditionné par une séquence d'entrée $u_i^{(k)}$ que nous notons (IOHMM) pour « Input Output Hidden Markov Model ». La variable exogène $u_i^{(k)}$ est une entrée permettant de modéliser des contraintes ou les variations de

l'environnement du composant. L'impact du processus caché sur les modes de défaillances est défini par la sortie $z_i^{(k)}$. Les variables $u_i^{(k)}$ et $z_i^{(k)}$ induisent le comportement du processus caché (non observable) $x_i^{(k)}$ décrivant la dégradation du composant (Ben Salem et al. 2006). Pour modéliser ce processus stochastique complexe $\mathbb{P}\left(z_i^{(k)} \middle| x_i^{(k)}, u_i^{(k)}\right)$, le formalisme des (IOHMM) est bien adapté (Bengio 1999 pp 145).



u1(k)	x1(k)	0	1	2
0	0	100,000	0,000	0,000
	1	0,000	100,000	0,000
	2	0,000	0,000	100,000
1	0	95,000	2,000	3,000
	1	0,000	100,000	0,000
	2	0,000	0,000	100,000
2	0	90,000	4,000	6,000
	1	0,000	100,000	0,000
	2	0,000	0,000	100,000

Figure 32 : Modèle RB Dynamique d'un MSM



x1(k+1)	0	1
0	100,000	0,000
1	0,000	100,000
2	0,000	100,000

Figure 33 : Modèle RB Dynamique d'un IOHMM

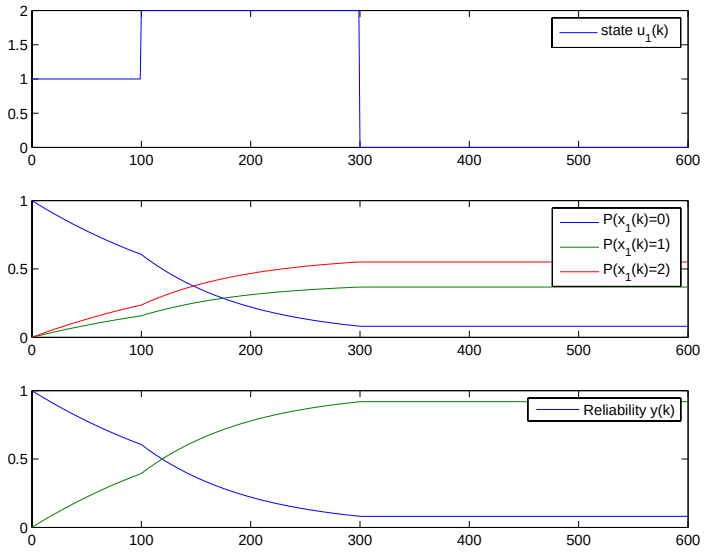


Figure 34 : Inférence du RB Dynamique du modèle IOHMM

Comme nous l'avons proposé (Ben Salem et al. 2006) la modélisation par un RBD d'un IOHMM appliquée à la fiabilité des composants est très simple (Figure 33). Dans le modèle IOHMM nous supposons que $u_i^{(k)}$ a trois états :

- '0' le composant n'est pas utilisé ;
- '1' le composant est utilisé dans des conditions normales d'utilisation ;

- ‘2’ le composant est utilisé en dehors des conditions normales d’utilisation.

Une simulation de l’évolution de la distribution de l’état du composant $x_i^{(k+1)}$ et de la fonction réalisée pas le composant $z_i^{(k+1)}$ est donnée pour une séquence de $u_i^{(k)}$ définie de $k = 0$ à $k = 600$ (Figure 34).

4.2 Modélisation d’un système multi-état dynamique

Un réseau bayésien dynamique devient particulièrement intéressant dès que plusieurs composants sont à prendre en compte dans la modélisation d’un système. Les RBD présentés dans la section 4.1 permettent de représenter plusieurs processus aléatoires multi-états distincts au sein d’un modèle du système. Un modèle multi-état, tel que nous l’avons présenté dans la section 3.2, permet facilement de fusionner les modèles de composants multi-états dynamiques de la section 4.1 pour former un modèle du système multi-état dynamique. Le calcul dans un RBD contenant plusieurs processus aléatoires n’est pas trivial. Des algorithmes d'inférence différents sont adaptés aux structures et aux conditions d’utilisation des modèles.

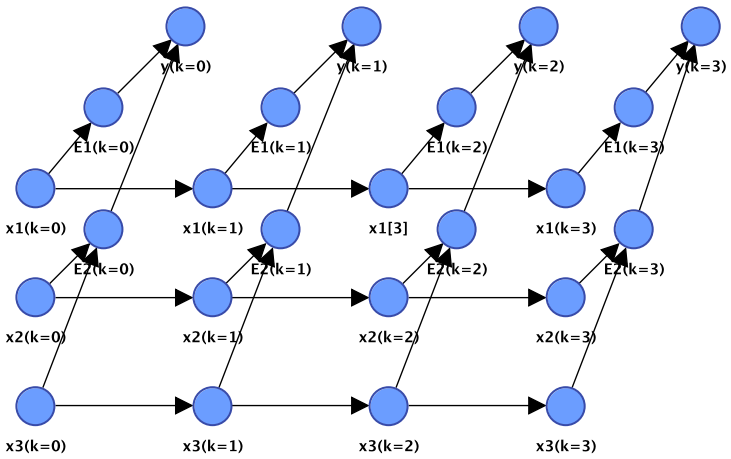


Figure 35 : Modèle RB Dynamique déroulé sans dépendance conditionnelle entre composants

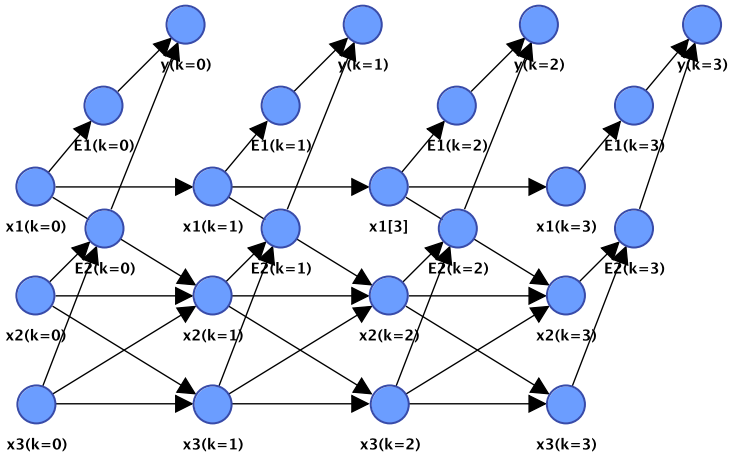


Figure 36 : Modèle RB Dynamique déroulé avec dépendance conditionnelle entre composants

Les algorithmes d'inférence exacte comme par exemple les algorithmes basés sur la construction d'un arbre de jonction (Jensen, 1996) s'appliquent pour les modèles déroulés. Si toutes les tranches de temps sont explicitées dans le modèle alors les algorithmes d'inférence classiques sont mis en œuvre pour calculer les résultats exacts (Figure 35). Les modèles peuvent être de complexité très grande avec des dépendances importantes entre les composants (Figure 36). Malheureusement comme nous l'avons expliqué précédemment cette modélisation n'est pas intéressante car elle ne permet pas de dérouler le modèle sur des horizons temporels très longs (quelques tranches de temps uniquement).

Dans le cas d'un modèle à *deux tranches de temps* (2TBN), la condition qui permet de garantir des calculs exacts est que les processus aléatoires modélisés sont indépendants. Cette condition est vérifiée dans certains cas par exemple si tous les composants sont indépendants comme dans le cas de la (Figure 37).

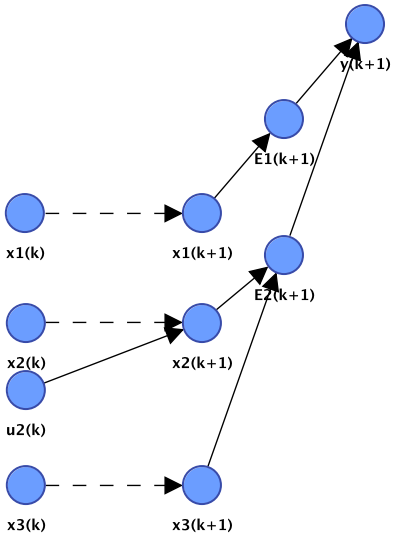


Figure 37 : Modèle RB Dynamique 2TBN d'un système multi-état

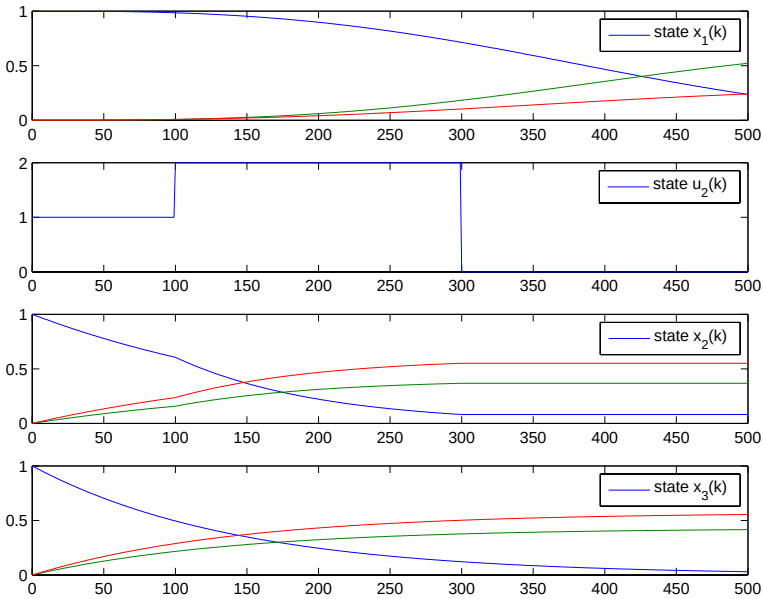


Figure 38 : Inférence dans le RB Dynamique 2TBN d'un système multi-état : distribution d'état des composants

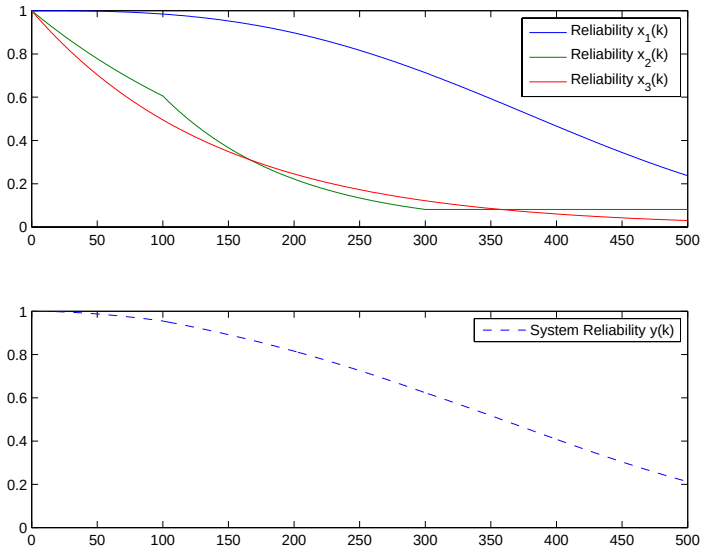


Figure 39 : Fiabilité des composants et du système multi-état

La distribution marginale est calculée facilement dans le 2TBN en utilisant un algorithme d'inférence exacte. Nous calculons alors la distribution de probabilité sur tous les composants multi-états (Figure 38). Pour le composant 1, nous faisons l'hypothèse d'un processus à paramètre non constant :

- La défaillance 1 (blocage fermé de la vanne) a une probabilité d'occurrence donnée par l'équation : $\lambda_{1Pf} = \frac{\beta \cdot k^{(\beta-1)}}{\alpha^{\beta}}$ avec $\beta = 3$ et $\alpha = 500$.
- La défaillance 2 (blocage ouvert de la vanne) a une probabilité d'occurrence donnée par l'équation : $\lambda_{1Po} = \frac{\beta \cdot k^{(\beta-1)}}{\alpha^{\beta}}$ avec $\beta = 2{,}5$ et $\alpha = 700$

Le composant 2 est défini conditionnellement à trois modes de fonctionnements définis par la variable $u_i^{(k)}$:

- $u_i^{(k)} = 0$ le composant n'est pas utilisé $\lambda_{2Pf} = 0$ et $\lambda_{2Po} = 0$;
- $u_i^{(k)} = 1$ le composant est utilisé dans des conditions normales d'utilisation $\lambda_{2Pf} = 2 \cdot 10^{-3}$ et $\lambda_{2Po} = 3 \cdot 10^{-3}$;
- $u_i^{(k)} = 2$ le composant est utilisé en dehors des conditions normales d'utilisation $\lambda_{2Pf} = 4 \cdot 10^{-3}$ et $\lambda_{2Po} = 6 \cdot 10^{-3}$.

Pour le composant 3 nous modélisons la chaîne de Markov (Figure 67) avec les probabilités de transitions suivantes $\lambda_{2Pf} = 3 \cdot 10^{-3}$ et $\lambda_{2Po} = 4 \cdot 10^{-3}$.

Ainsi, les composants indépendants sont modélisés dans un RBD soit par une Chaîne de Markov, une Chaîne de Markov non homogène, par MSM ou IOHMM indépendantes. Le RBD permet de formaliser le modèle du système multi-état constitué de composants indépendants sous une forme factorisée. Les processus sont représentés par le modèle RBD

de la (Figure 37). La tranche de temps $k+1$ permet de modéliser la propagation des états des composants vers la fonction principale du système (Figure 39).

Discussion sur le cas de non indépendance des processus

Malheureusement, les processus ne sont pas toujours indépendants. Pour diminuer la complexité du modèle dans le cas de processus non indépendants, il est possible de fusionner les composants dépendants dans un seul processus qui est ensuite combiné avec les autres processus indépendants par un RB multi-état. Selon cette méthode, la RB conduit à modéliser des processus stochastiques indépendants, la structure du modèle global du système est simplifiée, mais le nombre d'états par variable augmente.

Néanmoins, si des dépendances existent entre les processus aléatoires comme dans le modèle déroulé de la (Figure 36), il est nécessaire d'utiliser un algorithme d'inférence spécifique qui estime la distribution jointe à chaque pas de temps. L'algorithme d'inférence approximative (Boyen et Koller 1998 ou Koller et al. 1999) permet d'estimer la distribution marginale avec une erreur bornée. Il est aussi possible d'utiliser des méthodes d'inférence approximatives, comme utilisées pour le filtrage particulaire dans les méthodes MCMC par exemple (Koller et Lerner, 2000). De nombreux algorithmes d'inférences sont développés dans la littérature, je n'ai pas pour objectif de contribuer à l'amélioration de ces algorithmes. Les travaux de Laurent Bouillaut font état de différentes variantes d'algorithmes d'inférences (Bouillaut 2014).

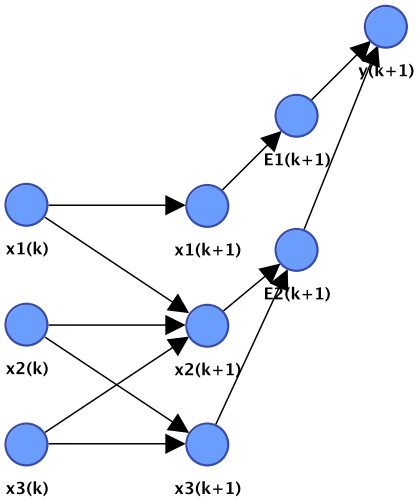


Figure 40 : Modèle 2TBN d'un système multi-état avec processus fortement dépendants

Malheureusement, un autre phénomène conduit à des difficultés dans le calcul de la distribution marginale, même pour la structure indépendante de la Figure 37. Dans l'analyse de scénarios de fonctionnement, il est intéressant d'intégrer des observations (événements) dans le RBD. Dans la (Figure 37), si une observation (évidence) est introduite sur un composant $x_i^{(k)}$ ou une variable exogène $u_i^{(k)}$ l'inférence ne pose pas de problème, les processus restent indépendants. Cependant si une observation est introduite sur une autre variable par exemple $y_i^{(k+1)}$ cette observation rend conditionnellement dépendantes les

variables $x_i^{(k+1)}$. Cette dépendance conduit à la nécessité d'utiliser des algorithmes d'inférence capables de la prendre en compte. Il est donc nécessaire de prendre des précautions dans l'utilisation de RBD et d'utiliser les algorithmes d'inférence appropriés en respectant les conditions de validité des hypothèses d'indépendances.

4.3 Conclusion

Nous avons montré que les Réseaux Bayésiens Dynamiques (RBD) permettent de diminuer l'effet de l'explosion combinatoire dans l'évaluation de fiabilité par une factorisation des processus d'un système multi-état (Weber et Jouffe 2003). Les RBD sont un formalisme de représentation des Chaînes de Markov (MC) (Weber et Jouffe, 2003), des Processus de Markov Cachés (HMM) et des Processus de Markov Cachés à entrée sortie (IOHMM). Ils sont bien adaptés à la modélisation de la fiabilité des composants (Weber et al., 2004 ; Ben Salem et al. 2006). Nous avons également proposé d'utiliser un RBD pour la modélisation de processus de Markov non homogènes en utilisant des paramètres variables dans le temps (Weber et al. 2004). Nous avons formalisé l'intégration de variables exogènes représentant des événements extérieurs dans un processus de dégradation en utilisant un processus MSM. L'originalité de nos propositions est de formaliser le processus de dégradation d'un composant et son interaction avec l'environnement par un modèle IOHMM (Ben Salem et al., 2006).

Les RBD sont un formalisme de modélisation de la fiabilité capable de modéliser le vieillissement des composants en intégrant l'impact des opérations de maintenance et de l'évolution de l'environnement opérationnel des composants. Dans les articles (Weber et Jouffe, 2006 ; Muller et al. 2004) nous proposons un modèle formalisé par Réseau Bayésien Dynamique pour l'analyse de la fiabilité et le pronostic d'un système. Le modèle formalisé par RBD est basé, d'une part sur un modèle probabiliste multi-état du système et d'autre part sur un modèle dynamique du comportement fiabiliste des composants.

Nous avons appliqué la modélisation par RBD dans l'aide à la décision en diagnostic (Weber et al. 2008). Dans ces travaux, un RBD intègre les modèles de fiabilité des composants au modèle de décision probabiliste pour le diagnostic de défauts. Nous avons également travaillé avec Sylvain Verron (Verron et al. 2008 et 2009) sur la classification par RB appliquée au diagnostic de défauts.

Les travaux développés dans la thèse (Ben Salem, 2008), traitent de la modélisation d'évènements organisés en séquences temporelles. Dans l'application traitée en partenariat avec l'INRETS[3], les évènements pris en compte correspondent à des caractéristiques structurelles du rail. Le but est de diagnostiquer des dégradations (fissures, écailles, usures

[3] INRETS Institut National de REcherche sur les Transports et leur Sécurité. Depuis 2011, l'INRETS et le LCPC ont fusionné pour donner l'IFSTTAR Institut Français des Sciences et Technologies des Transports, de l'Aménagement et des Réseaux.

ondulatoires) d'un réseau ferroviaire. Cette modélisation est réalisée par des RBD formalisant le processus stochastique sous la forme d'une IOHMM. Cette modélisation est utilisée pour l'estimation d'événements normaux, à dissocier des dégradations. Ce modèle de simulation est testé sur un problème concret de labellisation des points singuliers de l'infrastructure ferroviaire, en vue d'une aide à la classification de dégradation de rails (Bouillaut et al. 2004), (Ben Salem et al 2004). Ces travaux ont été poursuivis par Laurent Bouillaut (Samé et al. 2007 ; Oukhellou et al. 2008).

5 Intégration de la fiabilité à la commande de système

Comme nous l'avons décrit dans la partie précédente, les modèles probabilistes que nous développons sont appliqués en maîtrise des risques, en maintenance et en diagnostic. Mais les modèles probabilistes peuvent aussi être utilisés pour adapter les stratégies de contrôle-commande pour garantir la sécurité et la satisfaction des objectifs du système avant un arrêt normal du système ou une intervention de maintenance. Ainsi, nous proposons d'optimiser la loi de commande par rapport aux aléas dus à l'interaction du système avec son environnement et aux dégradations dues à l'usure des composants.

La stratégie de commande a un impact important sur les performances du système et leur maintien dans la durée. Par exemple, modifier une loi de commande en présence de dérives (défauts) dans le fonctionnement du système peut permettre de garantir les performances. Cependant, surcharger un actionneur pour compenser une dérive peut conduire à une dégradation plus rapide des composants du système, il en résultera une diminution de la performance à long terme.

Les modèles nécessaires pour estimer les dégradations conditionnellement aux changements des conditions opérationnelles doivent être utilisés en ligne durant la phase d'exploitation du système. Pour mener à bien ces activités de recherche, il est nécessaire de rechercher des formalismes de modélisation permettant d'évaluer (pronostiquer) les modes de fonctionnements résultants des situations qui apparaissent au cours du temps. De plus les méthodes de commande ne sont pas prévues pour intégrer des connaissances probabilistes issues des modèles de fiabilité. Il est nécessaire de définir des méthodes d'intégration de connaissances probabilistes dans les algorithmes de commande.

Cette action de recherche est en cours et nous n'avons pas encore résolu le problème. Mon objectif est d'appliquer les modèles RBD, présentés dans la section précédente, à l'estimation (le pronostic) de l'impact des événements environnementaux et du contexte d'utilisation des composants sur les performances du système à des fins d'améliorer la stratégie de commande et de restructuration ou reconfiguration dans un contexte de systèmes tolérants aux fautes et aux défaillances.

5.1 Revue des travaux faisant un lien entre fiabilité et commande

La dégradation des actionneurs et la fiabilité du système ont été examinées dans peu de travaux de recherche sur la commande des systèmes. Gokdere et al. (2005) propose d'intégrer des paramètres permettant de prolonger la durée de vie des actionneurs afin de réduire les coûts de maintenance. La méthode repose sur l'estimation du temps restant avant la défaillance de l'actionneur en fonction des conditions d'exploitation passées du composant, puis la modification de l'état de fonctionnement du composant si la durée de vie

restante estimée est inférieure à celle souhaitée. Les auteurs (Gokdere et al., 2006) ont présenté des algorithmes de commande adaptative, l'un conserve la durée de vie souhaitée de l'actionneur en adaptant son niveau de performance, l'autre offre un compromis entre la performance de l'actionneur et la durée de vie en fonction des besoins de la mission.

(Pereira et al., 2010) propose une solution basée sur une commande par un Modèle de Control Prédictif (MPC) utilisée pour répartir les charges entre les actionneurs redondants en imposant des contraintes sur la dégradation des actionneurs. La dégradation de l'actionneur est calculée par le cumul des commandes. Elle est intégrée comme contrainte dans une commande MPC garantissant de ne pas atteindre un niveau de dégradation de l'actionneur dangereux à la fin de la mission. Cette méthode n'est pas basée sur le calcul de la fiabilité mais intègre l'idée que les Co-variables (ici la commande) impactent la fiabilité des composants. Toutes ces recherches se focalisent sur le principe d'amélioration de la fiabilité des actionneurs indépendamment de la fiabilité du système.

Les premiers travaux de recherche que nous avons menés ont été focalisés sur la définition d'une structure combinant les composants pour former un système ayant une fiabilité résiduelle la plus grande possible à l'issue d'une défaillance. Les recherches menées dans la thèse (Guenab, 2007 ; Guenab et al., 2011), reposent sur l'amélioration de la commande tolérante aux défauts dont le principe est de maintenir les performances les plus proches possibles de celles définies avant l'apparition de défauts. La contribution réside dans le fait de proposer une stratégie de commande tolérante aux défauts (reconfiguration ou restructuration), basée sur l'analyse de la fiabilité et le coût des composants (Guenab et al., 2004a et 2004b). A l'issue de la détection et l'isolation d'un défaut dans le système, la tâche de la reconfiguration consiste à déterminer parmi toutes les structures possibles celles qui assurent les performances initiales du système ou des performances dégradées, en isolant des composants ou en basculant sur des parties non défaillantes. La méthode proposée repose sur l'obtention d'une structure optimale parmi l'ensemble des structures possibles (Guenab et al., 2005). L'approche est illustrée sur un système pilote défini dans le cadre du projet européen IFATIS (Guenab et al., 2004a, 2005, 2006).

Les travaux développés dans la thèse (Khelassi 2011) font suite à la thèse (Guenab, 2007). La thèse (Khelassi, 2011) propose une méthodologie de synthèse de lois de commande tolérante aux fautes garantissant la fiabilité des systèmes. Cette nouvelle méthodologie nécessite l'adaptation des différents modèles ou paramètres de la fiabilité pour les intégrer comme contrainte ou critère conditionnant la loi de commande. L'intégration explicite en ligne de l'impact de la charge dans les lois modélisant la fiabilité des actionneurs sur le reste de la mission, est un des points clés de cette thèse.

Une première partie des travaux est consacrée à l'analyse de la « reconfigurabilité » des systèmes tolérants aux fautes (Khelassi et al. 2009a, 2009b). Cette analyse de reconfigurabilité en présence de défauts est basée sur la consommation d'énergie ainsi que les objectifs de fiabilité du système sur le reste de la mission à l'issue de l'occurrence du défaut (Khelassi et al. 2010a). Un indice de reconfigurabilité est proposé définissant les limites fonctionnelles d'un système commandé en fonction de la sévérité des défauts et de la dégradation des actionneurs en terme de fiabilité (Khelassi et al. 2011a).

Nous avons travaillé sur le problème d'allocation de la commande. Des solutions sont développées en prenant en compte l'état de dégradation et du vieillissement des actionneurs (Khelassi et al. 2010b, 2011d, 2011e). Les entrées de commandes sont attribuées en fonction de la fiabilité des actionneurs et de l'occurrence des défauts (Khelassi *et al.* 2011b).

Nos derniers travaux se sont focalisés sur l'exploitation d'un modèle capable de représenter la fonction de structure du système pour pouvoir lier la fiabilité des composants à la fiabilité du système. Nous avons travaillé, durant la thèse (Khelassi 2011), sur la synthèse d'une loi de commande tolérante aux défauts garantissant la fiabilité globale du système. Une commande du système est proposée en se basant sur un calcul de sensibilité de la fiabilité du système par rapport aux actionneurs. Ainsi, une méthode de commande tolérante aux défauts en tenant compte de la criticité des actionneurs est synthétisée sous une formulation LMI (Khelassi et al. 2011c), (Khelassi et al. 2012).

Nos connaissances sur les RBD nous permettent aujourd'hui d'envisager l'intégration d'un modèle de fiabilité du système dans la commande d'un système continu (Weber et al 2012c). Dans nos récents travaux (Bicking et al 2013a, 2013b et 2014) nous avons travaillé sur l'intégration de la sensibilité de la fiabilité du système par rapport aux défaillances des composants. Nous avons utilisé un RBD pour intégrer l'impact de la charge sur la fiabilité des actionneurs sous la forme d'un processus stochastique à paramètres variant dans le temps en fonction de la charge. Notre objectif est d'intégrer la modélisation par RBD dans la commande des systèmes réels. Ce sont ces principes que la section suivante présente plus précisément.

5.2 Proposition de commande intégrant la fiabilité par une modélisation par Réseau Bayésien Dynamique

L'objectif de ces recherches est de définir une stratégie de commande pour des systèmes sur-actionnés permettant une répartition optimale des efforts sur les actionneurs en préservant la fiabilité globale du système dans le cas nominal ou en présence de défaillances d'actionneurs. Pour optimiser les commandes des actionneurs, il est nécessaire d'avoir suffisamment de degrés de liberté dans la loi de commande. C'est le cas des systèmes sur-actionnés. Un système sur-actionné n'est pas nécessairement un système ayant des composants en redondance matérielle, mais c'est un système pour lequel les objectifs de commande sont atteignables par plusieurs solutions.

Modélisation et commande d'un système sur-actionné

D'un point de vue général, nous considérons un système sur-actionné comme un système linéaire avec m actionneurs décrit par l'équation d'états discrets suivante :

$$\begin{cases} \tilde{x}(k+1) = A\tilde{x}(k) + B_u\tilde{u}(k) \\ \tilde{y}(k+1) = C\tilde{x}(k) \end{cases} \quad (10)$$

Avec $A \in \mathbb{R}^{n\times n}$, $B_u \in \mathbb{R}^{n\times m}$ et $C \in \mathbb{R}^{p\times n}$ respectivement les matrices d'état, de contrôle et de sortie. $\tilde{x} \in \mathbb{R}^n$ est le vecteur d'état du système, $\tilde{u} \in \mathbb{R}^m$ est le vecteur de commande du système et $\tilde{y} \in \mathbb{R}^p$ est le vecteur de sortie du système. La condition : $rank\ (B_u) = r < m$

caractérise les systèmes sur-actionnés. La (Figure 41) présente le principe de commande d'un système sur-actionné intégrant la fiabilité. Le modèle de fiabilité du système est utilisé pour répartir les efforts de commande $\tilde{u}(k)$ sur les actionneurs.

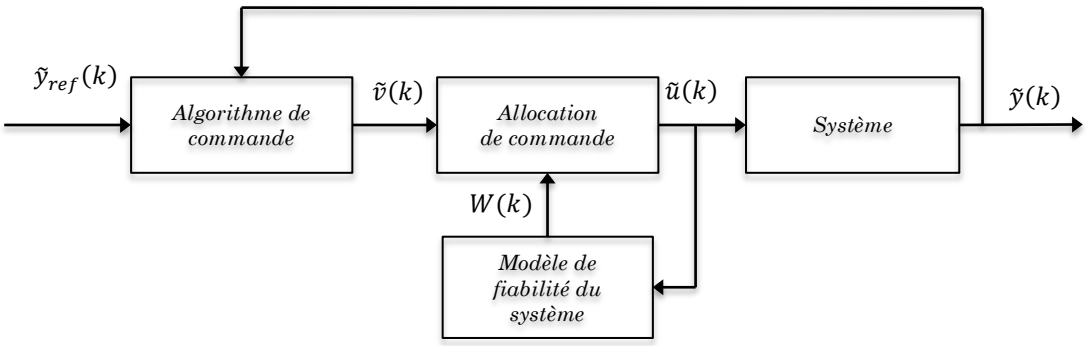


Figure 41 : Structure de commande d'un système sur-actionné intégrant un modèle de fiabilité

La matrice B_u peut être factorisée :

$$B_u = B_v B \tag{11}$$

Avec $B_v \in \mathbb{R}^{n\times r}$ et $B \in \mathbb{R}^{r\times m}$ tous deux de rang r. Le système est modélisé alors par :

$$\begin{cases} \tilde{x}(k+1) = A\tilde{x}(k) + B_v\tilde{v}(k) \\ \tilde{v}(k) = B\tilde{u}(k) \\ \tilde{y}(k+1) = C\tilde{x}(k) \end{cases} \tag{12}$$

Avec $\tilde{v}(k) \in \mathbb{R}^r$ représentant l'ensemble des efforts de commande nécessaire au fonctionnement du système. $\tilde{v}(k)$ est aussi appelé le vecteur d'entrée virtuelle. L'allocation de commande a pour objectif de définir les commandes $\tilde{u}(k)$ réelles du système à partir de la commande virtuelle désirée telle que :

$$\begin{gathered} \tilde{v}^d(k) = B\tilde{u}(\mathrm{k}) \\ \tilde{u}_{min} \le \tilde{u} \le \tilde{u}_{max} \end{gathered} \tag{13}$$

$\tilde{v}^d(k)$ est calculé par un algorithme de commande pour satisfaire des objectifs de régulation et de poursuite. $\tilde{u}_{min} \le \tilde{u} \le \tilde{u}_{max}$ représente les limites physiques de saturation des actionneurs.

Une solution au problème d'allocation de commande est donnée par résolution d'un problème d'optimisation. S'il n'existe pas de solution, une solution optimale de commande est définie dans les limites de $\tilde{u}(k)$ tel que $B\tilde{u}(k)$ donne la meilleure approximation de $\tilde{v}^d(k)$. La commande optimale peut être obtenue par la minimisation des critères suivants :

$$\Psi = \underset{\tilde{u}_{min}\le\tilde{u}\le\tilde{u}_{max}}{\arg min}\ \frac{1}{2}\|B\tilde{u}(k) - \tilde{v}^d(k)\|_2 \tag{14}$$

$$\tilde{u}(k) = \underset{\tilde{u}\in\Psi}{\arg min}\|W(k)(\tilde{u}(k) - \tilde{u}^d(k))\|_2 \tag{15}$$

Avec Ψ l'ensemble des solutions possibles pour la commande $\tilde{u}(k)$ en accord avec les objectifs du contrôleur ; et $\tilde{u}^d(k)$ est la commande désirée.
La matrice $W(k) \in \mathbb{R}^{m\times m} \succ 0$ permet de donner des niveaux de priorité à l'ensemble des actionneurs. $W(k)$ est défini classiquement sous une forme diagonale :

$$W(k) = \text{diag}([w_1(k)\ w_2(k)\ \cdots w_i(k) \cdots w_m(k)]) \tag{16}$$

Intégration de la fiabilité

La matrice de pondération $W(k)$ est considérée comme une clé pour intégrer la fiabilité des actionneurs dans le problème d'allocation de commande des systèmes sur-actionnés. Le problème de commande que nous proposons est résolu en plusieurs étapes, comme le présente la Figure 42.

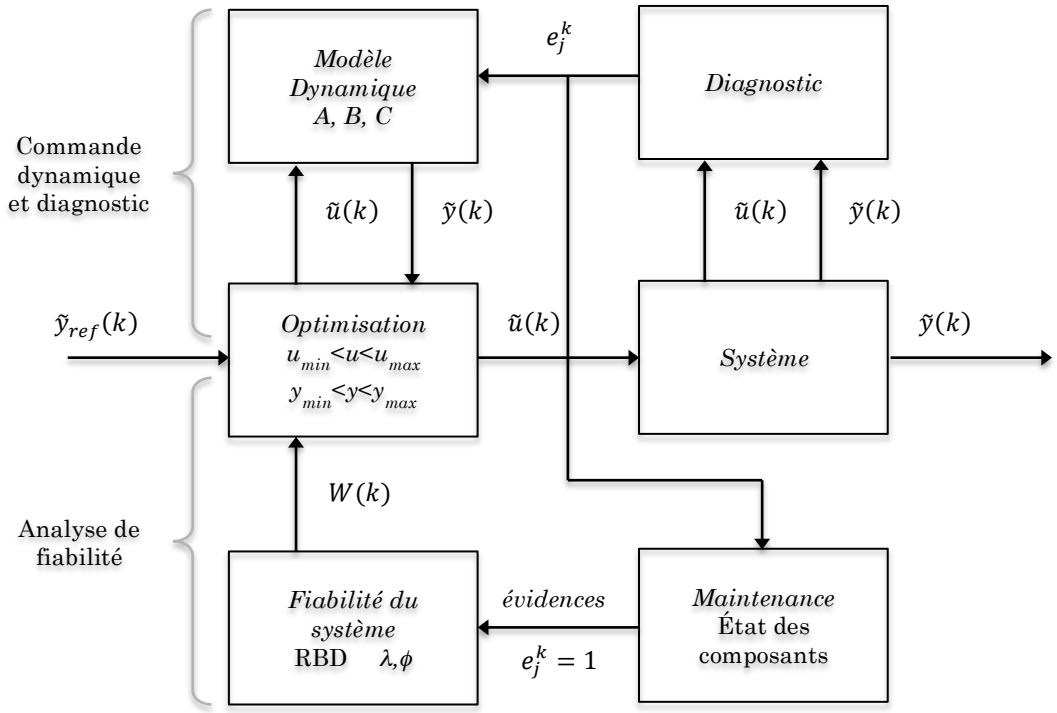


Figure 42 : Structure de commande d'un système sur-actionné intégrant un modèle de fiabilité par RBD

Afin d'améliorer la fiabilité du système, nous avons proposé de définir la matrice de pondération $W(k)$ à partir de la contribution α_i^k des actionneurs au fonctionnement du système :

$$\mathbb{P}(\alpha_i^k = 0) \tag{17}$$

Cette contribution dépend de la fonction de structure $\phi(e^k)$ où $e^k = \left(e_1^k, e_2^k, \ldots, e_m^k\right)$ qui permet de calculer la fiabilité du système en fonction des états de fonctionnement des actionneurs e_i^k.

Les actionneurs sont pris en compte dans la stratégie de contrôle proportionnellement à leur contribution au fonctionnement du système. L'état du système S^k est défini à partir de la

fonction de structure $\phi(e^k)$:

$$\mathbb{P}(S^k = 0) = \mathbb{P}(\phi(e^k) = 0) \quad (18)$$

Du point de vue de la commande, par hypothèse, le système sur-actionné est dans un état de fonctionnement même si certains actionneurs sont hors d'usage $e_j^k = 1$. Les actionneurs à utiliser, pour atteindre les objectifs du système, dépendent de la disponibilité des actionneurs et de la fonction de structure du système ϕ.

Les actionneurs indisponibles $e_j^k = 1$ sont définis par la fonction « *Maintenance* » de la (Figure 42) à partir d'une fonction « *Diagnostic* ». Un actionneur e_i^k disponible est utilisé par la loi de commande s'il existe au moins un scénario de fonctionnement $\phi(e^k) = 0$ contenant e_i^k. La probabilité d'utiliser un actionneur et de satisfaire les objectifs du système est définie par la probabilité conditionnelle suivante :

$$\mathbb{P}\left(\alpha_i^k = 0 | \phi(e^k) = 0\right) \quad (19)$$

Afin d'intégrer la fiabilité des actionneurs dans la stratégie de commande, la matrice de pondération $W(k)$ est estimée en ligne en fonction de l'indisponibilité des actionneurs donnée par la fonction « *Diagnostic* ». Par conséquent, si un actionneur e_j^k est indisponible $e_j^k = 1$, le système peut fonctionner en mode dégradé car il est sur-actionné et le scalaire $w_i(k)$ de chaque actionneur est défini par la probabilité suivante :

$$w_i(k) = \mathbb{P}\left(\alpha_i^k = 0 | \phi(e^k) = 0, e_j^k = 1\right) \quad (20)$$

Le poids $w_i(k)$ correspond à la probabilité de contribution de l'actionneur e_i^k lorsque le système fonctionne compte tenu de l'indisponibilité de certains actionneurs défaillants. L'évaluation de cette probabilité n'est pas uniquement basée sur la santé de l'actionneur mais considère la structure du système et la disponibilité de tous les autres actionneurs.

En utilisant une modélisation de fiabilité standard, l'évaluation de cette probabilité est complexe (voir même impossible selon la structure ϕ), mais ce calcul est facilement réalisé grâce au mécanisme d'inférence des RBD.

5.3 Application à un système de distribution d'eau potable

La méthode présentée précédemment est appliquée sur un réseau de distribution d'eau potable (RDEP). Un réseau de distribution d'eau est un système sur-actionné car plusieurs chemins permettent d'acheminer l'eau entre les sources et les utilisateurs. Le débit à travers ces voies est commandé au moyen d'actionneurs tels que des pompes et des vannes.

Grâce à une collaboration internationale, une partie du réseau de distribution d'eau potable de Barcelone (Espagne) a été utilisé comme plate-forme d'illustration (Figure 43). Le réseau dispose d'un système de télé-contrôle centralisé, organisé dans une architecture à deux niveaux. Au niveau supérieur, un système de contrôle et de surveillance est installé dans le centre de contrôle (Agbar). Ce système est en charge du contrôle de l'ensemble du réseau en tenant compte des contraintes opérationnelles et des exigences des consommateurs.

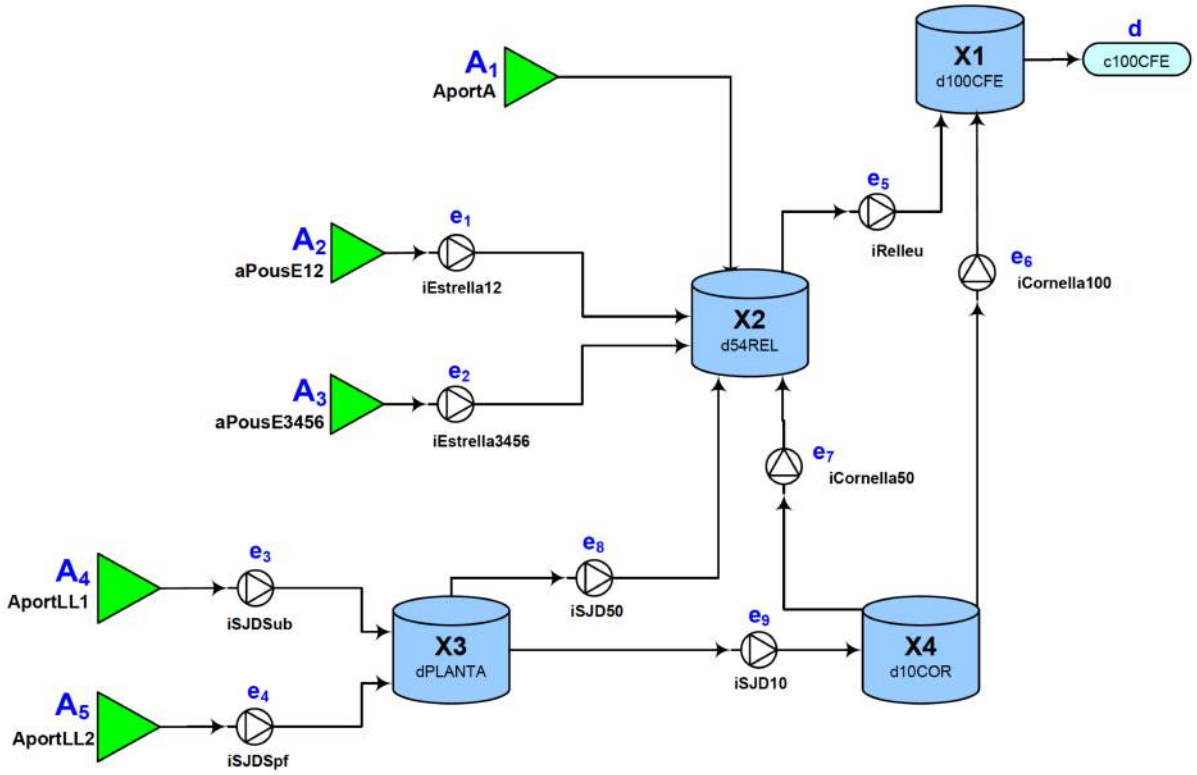


Figure 43 : Partie du RDEP de Barcelone étudié

Tableau 21

Variable	Nom de l'actionneur	taux de défaillance (10^{-4})
e_1	iEstrella12	1,2
e_2	iEstrella3456	3,456
e_3	iSJDSub	6,3
e_4	iSJDSpf	9,5
e_5	iRelleu	1
e_6	iCornella100	10
e_7	iCornella50	5
e_8	iSJD50	5
e_9	iSJD10	1

Tableau 22

Variable	Pondération de l'actionneur
α_{e1}	WiEstrella12
α_{e2}	WiEstrella3456
α_{e3}	WiSJDSub
α_{e4}	WiSJDSpf
α_{e5}	WiRelleu
α_{e6}	WiCornella100
α_{e7}	WiCornella50
α_{e8}	WiSJD50
α_{e9}	WiSJD10

Un RDEP est un système de réseau de flux qui relie des sources (approvisionnement en eau), et des demandes (secteurs de demandes en eau) par des canalisations. Il contient également des éléments actifs tels que les pompes et les vannes. Dans nos travaux, pour l'étude de la fiabilité du RDEP, les sources, les réservoirs et les canalisations sont considérés comme parfaitement fiables et sans saturation. Seuls les éléments actifs sont considérés comme n'étant pas parfaitement fiables.

Nous avons appliqué la méthode en simulation sur cinq sources d'eau potable et une demande comme le présente la (Figure 43). Pour répondre à la demande $d = y_{ref}(k)$ (C100CFE), au moins 2 des 5 sources (AportLL1, AportLL2, ApousE12, ApousE3456, Aporta) sont nécessaires pour satisfaire la quantité maximum journalière des consommateurs.

Tableau 23

Variable	Chemins
P_1	{AportLL2, iSJDSpf, iSJD10, iCornella100}
P_2	{AportLL1, iSJDSub, iSJD10, iCornella100}
P_3	{AportLL2, iSJDSpf, iSJD10, iCornella50, iRelleu}
P_4	{AportLL1, iSJDSub, iSJD10, iCornella50, iRelleu}
P_5	{AportLL2, iSJDSpf, iSJD50, iRelleu}
P_6	{AportLL1, iSJDSub, iSJD50, iRelleu}
P_7	{ApousE12, iEstrella12, iRelleu}
P_8	{ApousE3456, iEstrella3456, iRelleu}
P_9	{Aporta, iRelleu}

Modélisation par RBD

Toutes les sources sont supposées totalement disponibles. La distribution des temps de défaillance de tous les actionneurs est considérée exponentielle et les taux de défaillances sont donnés dans le (Tableau 21). Tous les chemins reliant les sources (AportLL1, AportLL2, ApousE12, ApousE3456, Aporta) à la demande (C100CFE) sont détaillés dans le (Tableau 23).

Le modèle de fiabilité par RBD est donné à la (Figure 44). Les variables P_i modélisent la disponibilité des chemins reliant les sources à la demande. Les variables A'_i définissent la disponibilité des sources à travers le RDEP en fonction de la disponibilité des chemins. La disponibilité du système est définie par la variable $S_{C100CFE}$. Les variables permettant le calcul des pondérations $w_i(k)$ sont définies dans le (Tableau 22).

Résultats et commentaires

Une simulation a été effectuée sur une durée de 3600 heures en utilisant Matlab pour mettre en œuvre la méthode fondée sur l'optimisation de la commande et de la fiabilité du RDEP. La partie RBD est modélisée avec la toolbox « Bayes Net Toolbox » (BNT) pour Matlab proposée par Kevin Murphy 2002.

Le résultat de simulation présenté dans la (Figure 45) montre la fiabilité de chaque actionneur et la fiabilité du RDEP. La fiabilité des actionneurs a une forme exponentielle décroissante alors que la fiabilité du système a une forme plus complexe car elle est issue de la combinaison des fiabilités des actionneurs et de la structure ϕ du système.

La (Figure 46) représente les commandes $\tilde{u}_i(k)$ appliquées aux actionneurs et les pondérations utilisées pour l'optimisation. Les courbes $\alpha_i(k)$ représentent la valeur des poids $w_i(k) = \mathbb{P}\left(\alpha_i^k = 0 | \phi(e^k) = 0, e_j^k = 1\right)$ en fonction de la fiabilité des composants, de la disponibilité des chemins permettant la connexion des sources à la demande et de l'état d'éventuels composants hors d'usage ou en réparation. Chaque pondération $w_i(k)$ est intégrée dans la diagonale de la matrice $W(k)$ pour l'optimisation et le calcul de $\tilde{u}(k)$.

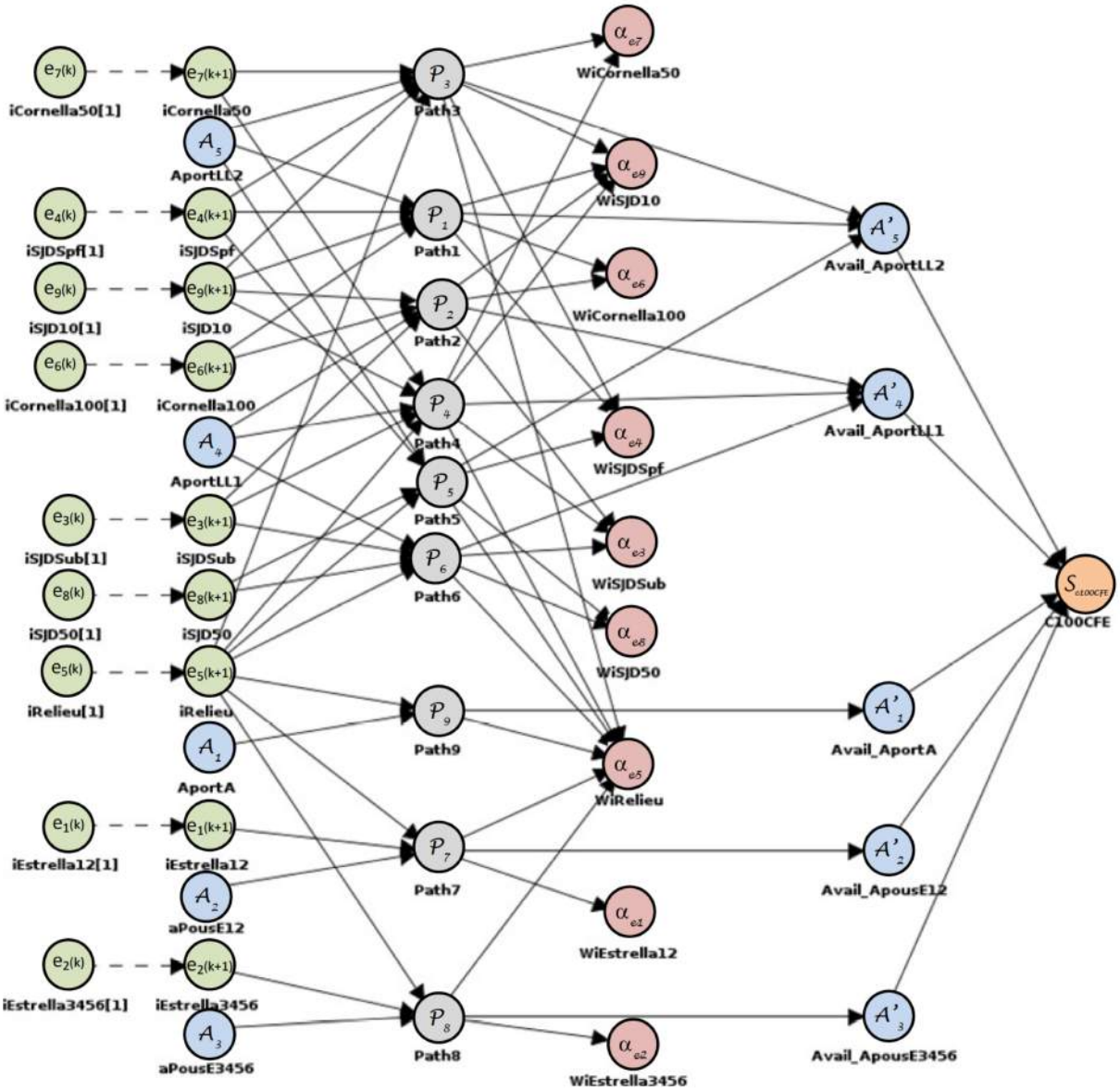


Figure 44 : Modèle RBD du système RDEP de Barcelone

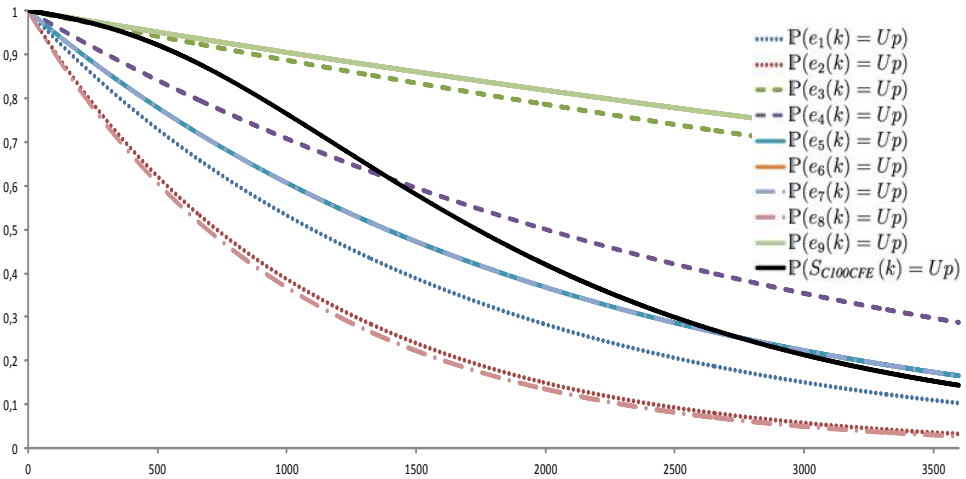


Figure 45 : Fiabilité a priori des actionneurs et du RDEP

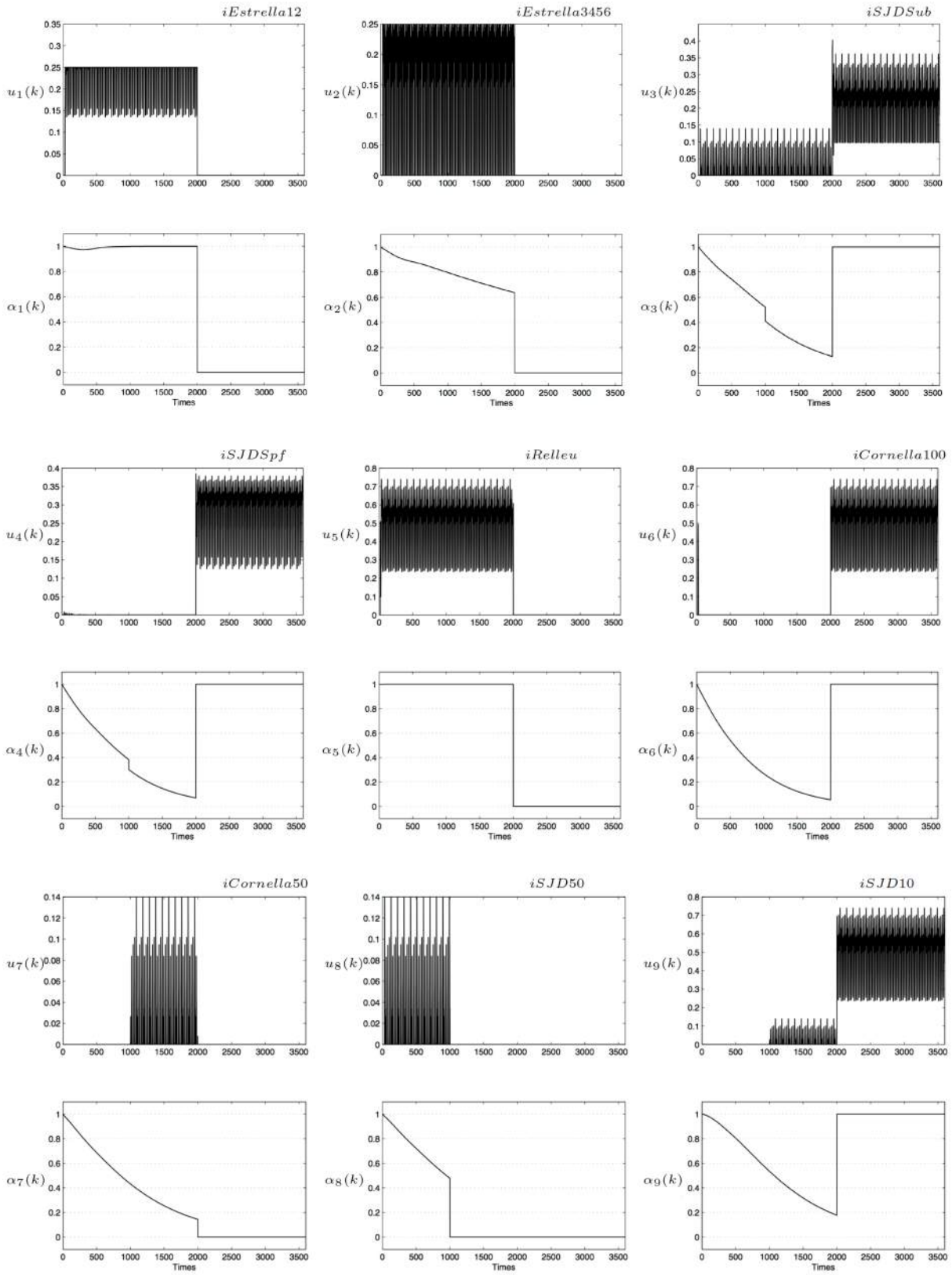


Figure 46 : Simulation des actions de commande et des pondérations du RDEP de Barcelone

Le scénario de simulation est divisé en 3 phases :

- Pour la phase 1, un cas sans défaillance des stations de pompage mais avec la source (Aporta) indisponible, est simulé de $(k = 0)$ à $(k = 1000)$. Dans ce cas (ApousE12) est facilement disponible par le chemin P_7 avec les composants e_5 (iRelleu) et e_1 (iEstrella12) qui sont les actionneurs les plus fiables. Les chemins P_7 et P_8 sont utilisés pour satisfaire à la demande. Les commandes $\tilde{u}_1(k)$ et $\tilde{u}_2(k)$ sont donc utilisées au maximum de leur capacité. Malheureusement une saturation des actionneurs e1 et e2 ne permet pas de satisfaire les pics de demandes journaliers. C'est donc $\tilde{u}_3(k)$ et $\tilde{u}_8(k)$ qui sont sollicités pour compenser les saturations de $\tilde{u}_1(k)$ et $\tilde{u}_2(k)$. Le passage par e_5 est privilégié car ce composant est plus fiable que e_6. C'est donc le chemin P_6 qui est privilégié. Le fonctionnement du RDEP est basé sur les chemins P_6, P_7 et P_8.
- Pour la phase 2, une panne critique est simulée sur la pompe e_8 (iSJD50) à $(k = 1000)$. Une fonction de «Diagnostic» est supposée mener à bien les tâches de détection de défaut et d'isolement. Le RBD permet de calculer les différents poids de l'actionneur $w_i(k)$ en intégrant que le composant e_8 est indisponible. Dans la (Figure 46) la courbe $\alpha_8(k)$ passe à zéro. Le chemin P_6 n'est plus utilisable la commande bascule alors sur le chemin P_4, les actionneurs e_7 et e_9 qui n'étaient pas utilisés jusqu'à présent sont alors mis en marche. Entre $(k = 1000)$ et $(k = 2000)$ les composants utilisés sont e_1, e_2, e_3, e_5 et e_7, e_9. Les commandes correspondantes sont donc différentes de 0.
- Pour la phase 3, à $(k = 2000)$ une seconde panne critique est simulée sur la pompe e_5 (iRelleu). La stratégie de commande privilégiant e_5 n'est plus valable, les chemins P_4, P_7 et P_8 ne sont plus utilisables. Par conséquent, le RBD détermine les pondérations $\alpha_1(k)$, $\alpha_2(k)$, $\alpha_5(k)$, $\alpha_7(k)$ égales à 0 en plus de la pondération $\alpha_8(k)$. Seuls les chemins contenant e_6 (iCornella100) sont utilisables, c'est-à-dire P_1 et P_2. Le système est alors reconfiguré pour fonctionner avec les composants e_3, e_4, e_6 et e_9. (Le RBD calcule les pondérations $\alpha_3(k)$, $\alpha_4(k)$, $\alpha_6(k)$ et $\alpha_9(k)$ égale à 1 car il n'y a pas d'autre scénario de fonctionnement possible.)

5.4 Conclusion

Dans cette section, nous avons proposé une méthode intégrant un RBD modélisant la fiabilité d'un système et de ses actionneurs dans une boucle d'optimisation de répartition des commandes sur les actionneurs d'un système.

Nous avons formalisé chaque étape du processus. Cette commande combine une répartition des charges sur un ensemble d'actionneurs pondéré par la fiabilité des actionneurs et leur contribution au fonctionnement du système. Il ne s'agit pas seulement de préserver la santé des actionneurs mais aussi de garantir la disponibilité de l'ensemble du système.

Cette stratégie de commande originale est mise en œuvre à la fois dans la situation nominale et en présence de défaillances d'actionneurs. Ces travaux de recherche sont encore à développer, mais les résultats que nous avons obtenus sont encourageants. Cet axe de recherche est un axe que je développe à court terme dans mon projet de recherche.

6 Conclusion sur mes activités de recherche

Malgré la maturité du formalisme des Réseaux Bayésiens permettant leurs exploitations dans des problèmes industriels et opérationnels, il est nécessaire de formaliser des démarches ou des méthodologies de construction et de structuration du modèle. En effet, comme les données ne sont pas disponibles pour un apprentissage automatique du modèle, un effort important doit porter sur la structuration des connaissances et la construction du modèle car la robustesse du modèle repose sur le bien-fondé et la justesse de la méthodologie de modélisation.

Les modèles structurés sous forme de graphes tels que les réseaux bayésiens devraient faire partie du panel des méthodologies incontournables de la maîtrise des risques et de la sûreté de fonctionnement. A travers les différents travaux de thèses et collaborations avec un ensemble de chercheurs, j'ai exploité des formalismes de modélisation permettant de structurer des modèles probabilistes fondés sur : les lois de fiabilité (Khelassi et al. 2011, Guenab et al. 2011, Weber et al. 2012a), les Chaînes de Markov (Pour et al. 2009), les Réseaux Bayésiens (Léger et al. 2008, Léger et al. 2009, Duval et al. 2012), les Réseaux Bayésiens Dynamiques (Weber et Jouffe 2003, Weber et Jouffe 2006, Weber et al. 2008), les Réseaux de Fonctions de Croyance (Simon et al. 2007, Simon et al. 2008, Simon et Weber 2009a, 2009b, Fallet-Fidry et al. 2012a, 2012b) ainsi que des Modèles Relationnels Probabilistes (Medina-Oliva 2013 et 2015). Ces méthodes ont été appliquées dans différents domaines de la sûreté de fonctionnement des systèmes.

Nous avons proposé des contributions dans les domaines de l'automatique continue :

- Le diagnostic de systèmes dynamiques pour analyser des résidus et intégrer des connaissances de fiabilité à la décision de localisation de défauts (Weber et al. 2008) ;
- La commande tolérante aux défauts pour le choix de structure de fonctionnement après détection et localisation de défauts (Guenab et al. 2005, 2011) ;
- L'analyse de reconfigurabilité des systèmes sous contrainte de fiabilité (Khelassi et al. 2009b, 2011) ;
- L'allocation de commande des systèmes sur-actionnés en présence de défauts ou en fonctionnement normal en fonction des caractéristiques de fiabilité des composants (Khelassi et al. 2010a, 2010b) ;
- L'analyse de fiabilité des systèmes tolérants aux défauts (Pour et al. 2009, Weber et al. 2012c) ;
- La synthèse de loi de commande avec pour objectif l'optimisation de la fiabilité du système en intégrant la sensibilité de la fiabilité du système par rapport aux composants dans le calcul des commandes (Bicking et al. 2013a et 2013b). Une formulation LMI est mise en œuvre pour obtenir le compromis stabilité-rapidité-fiabilité (Khelassi et al. 2011a, 2011b).

De plus, nous avons proposé des contributions à l'application et la structuration des modèles probabilistes pour :

- La modélisation de la fiabilité des composants en intégrant l'impact de l'environnement et des contraintes de fonctionnement (Weber et al. 2004, Ben Salem et al. 2006) ;
- La modélisation de la fiabilité de systèmes ayant une fonction de structure complexe

telle que la redondance K/n, K/n consécutif (Weber et al. 2010, Weber et Simon 2012, Simon et al. 2012) ;

- La modélisation de l'impact de la fiabilité et de la dégradation des composants sur les niveaux fonctionnels des systèmes (Weber et al. 2001a, Weber et Jouffe 2006, Medina-Oliva et al. 2013 et 2015) ;
- La modélisation de la fiabilité des systèmes en présence d'incertitudes épistémiques pour des fonctions de structure complexe (Simon et al. 2007, 2008, Simon et Weber 2009a, 2009b) ;
- La modélisation en maîtrise des risques de système complexe avec l'intégration de connaissances techniques, humaines et organisationnelles (Léger et al 2009, Duval et al. 2012) ;
- La modélisation en maîtrise des risques pour la prise en compte de l'incertitude épistémique et des connaissances incomplètes exprimées par les experts (Fallet et al. 2010, 2011, 2012, Fallet-Fidry et al. 2012a, 2012b) ;
- La modélisation probabiliste appliquée à l'évaluation de stratégies de maintenance pour des modèles intégrant des connaissances techniques, organisationnelles, logistiques, humaines, environnementales permettant le calcul d'indicateurs clés pour comparer des stratégies de maintenance (Medina-Oliva et al. 2013, 2011, 2010, 2009b).

Les apports majeurs de mes contributions se déclinent en 3 points :

Une modélisation des conséquences fonctionnelles des défaillances, structurée à partir des connaissances métiers :

Les principes de modélisation que nous avons développés sur la base des réseaux bayésiens permettent de relier la fiabilité et les effets des états de dégradation des composants à l'architecture fonctionnelle du système. Dans mon travail de recherche, les composants et les modes de défaillances sont alors décrits naturellement par des variables multi-états, par exemple issues des analyses AMDEC ou HAZOP, ce qui est difficile à modéliser par d'autres méthodes (Weber et al. 2001a, Weber et Jouffe 2006).

Nous proposons de représenter le modèle selon différents niveaux d'abstraction en relation avec les connaissances issues d'outils d'analyse fonctionnelle comme SADT (Structured Analysis and Design Technique) connues aussi sous le label IDEF0 (Integration Definition for Function modeling). Les répercussions (probabilistes) des défaillances sont propagées sur les fonctions du système en faisant apparaitre leur impact en terme de réalisation de la fonction ou d'apparition d'altération de la fonction ou de modes de défaillance (Weber et al. 2001a, Weber et Jouffe 2006, Medina-Oliva et al. 2013).

L'approche de modélisation par PRM est très intéressante car elle permet l'élaboration de modèles à partir de structures élémentaires. Grâce à cette flexibilité, la construction d'un modèle avec différents niveaux d'abstraction est facilitée. Les capacités des PRM permettent de capitaliser la connaissance par la création des classes génériques qui doivent être instanciées sur un système en particulier. Nous proposons ainsi de construire les modèles sur le principe des composants pris sur

étagère (commercial off-the-shelf ou COTS) (Medina-Oliva et al., 2009b).

Les algorithmes d'inférence dans le PRM facilitent le calcul des modèles de grande taille et des systèmes complexes. L'utilisation de la notion de classe permet d'établir des motifs probabilistes ou des fragments de réseau à travers la définition d'une famille d'objets partageant des propriétés communes : graphe, attributs, références et relations probabilistes. C'est un formalisme de modélisation qui devrait devenir incontournable en sûreté de fonctionnement.

Une modélisation dynamique de la fiabilité des systèmes basée sur la fiabilité des composants pris dans leur environnement :

Nous avons contribué lors de notre collaboration avec Bayesia à la modélisation de la fiabilité des systèmes par RBD. Comme nous l'avons illustré un RBD permet, grâce à la factorisation de la loi jointe, une complexité nettement inférieure à une Chaîne de Markov ainsi qu'un paramétrage bien plus facile à réaliser. La collaboration avec la société Bayesia a permis l'intégration dans Bayesialab (outil de modélisation RB) de ces extensions et notamment l'utilisation de paramètres variables dans le temps ce qui élargit le pouvoir de modélisation des RBD à des processus Markoviens non homogènes (Weber et al. 2004).

La prise en compte dynamique des variables contextuelles (Weber et al. 2004), représentant des contraintes exogènes, permet d'augmenter le pouvoir de modélisation des RBD à des structures équivalentes à des MSM (Markov Switching Model), HMM (Hidden Markov Model) et IOHMM (Input-Output Hidden Markov Model), que nous avons exploitées dans le cadre de modélisation de la fiabilité des composants (Ben Salem et al. 2006). Cette représentation correspond naturellement aux phénomènes que nous rencontrons en fiabilité. Les états des composants ne sont pas observables, seules les conséquences de la dégradation du composant sont visibles à travers les modes de défaillances qui apparaissent dans l'arborescence fonctionnelle de système.

Ce type de modélisation s'applique très bien dans le cas de modèle de pronostic (Muller et al. 2004). Dans le cas dynamique, nous proposons une modélisation par RBD qui relie le modèle de la fiabilité dynamique des composants prenant en compte le vieillissement (taux de défaillances variant dans le temps), avec les fonctions du système (Muller et al. 2004). Les modèles ainsi obtenus sont de grandes tailles et nous avons proposé d'utiliser un Réseau Bayésien Dynamique Orienté Objet (RBDOO) (Weber et Jouffe 2006) pour faciliter la construction et la maintenance du modèle.

La synthèse de la loi de commande avec pour objectif l'optimisation de la fiabilité du système basée sur sa sensibilité aux défaillances des actionneurs :

Nous travaillons depuis longtemps sur l'intégration de la fiabilité dans les objectifs de commande des systèmes sous contrainte de défaillances ou de défauts. Nos travaux ont porté initialement sur des analyses de fiabilités focalisées sur les actionneurs. Nous posons aujourd'hui le problème dans un contexte plus général de commande. Nous proposons une structuration du système de commande intégrant des fonctions d'optimisation et des fonctions d'évaluation de grandeurs probabilistes liées à la

fiabilité des composants et du système. Nos travaux récents sont focalisés sur l'intégration des facteurs d'importance comme paramètre de l'optimisation de la commande. La sensibilité de la fiabilité du système à la dégradation des actionneurs due aux surcharges engendrées par la commande est une clé pour l'allocation des efforts de commande. Cette direction est celle qui donne les meilleurs résultats. Nous sommes les premiers à exploiter cette idée sur cette thématique de recherche, l'intérêt croissant de la communauté scientifique nous conforte dans cette direction de recherche. C'est un axe de recherche à fort potentiel scientifique et applicatif pour les années à venir.

D'une manière générale, mes contributions tendent vers une formalisation de modèles probabilistes de grandes dimensions avec des vues fonctionnelles et dysfonctionnelles des systèmes en formalisant l'impact de l'environnement de fonctionnement et de conduite du système. Ceci répond bien aux problèmes actuels des industriels qui doivent intégrer de plus en plus de paramètres dans les analyses pour répondre à des demandes et directives gouvernementales de sécurité.

Chapitre 4

Projet de recherche

Mon projet de recherche s'inscrit dans la continuité de mes activités avec des évolutions selon trois axes : l'intégration de connaissances probabilistes dans la stratégie de commande des systèmes dynamiques ; la modélisation probabiliste en maîtrise des risques des systèmes sociotechniques et leurs impacts sur le développement durable et enfin la formalisation de modèles graphiques probabilistes en sûreté de fonctionnement pour de nouvelles classes de systèmes.

A court terme je souhaite renforcer mes activités de recherche sur l'intégration de la fiabilité dans la commande des systèmes tolérants aux défaillances. Cette activité de recherche conduit à résoudre plusieurs problèmes liés à la formalisation de modèles graphiques probabilistes dynamiques et leur exploitation dans une boucle d'optimisation ayant pour objectif d'estimer les commandes à appliquer aux systèmes afin d'en augmenter la fiabilité. Cette activité pourra être pérennisée à plus long terme dans une problématique plus large d'intégration de connaissances probabilistes dans la stratégie de commande des systèmes dynamiques.

Je souhaite à moyen terme orienter mes recherches en maîtrise des risques vers l'intégration de la résilience humaine dans la modélisation et à plus long terme l'extension de l'analyse à l'évaluation de conséquences économiques, sociétales et environnementales. Ceci correspond à un transfert de mes connaissances de modélisation vers la problématique du développement durable qui est aussi un des axes que je développe dans mes activités d'enseignement. La modélisation par Modèle Graphique Relationnel (PRM) est la voie que je souhaite développer pour supporter cette extension.

A plus court terme j'envisage de chercher des solutions de modélisation pour évaluer la sûreté de fonctionnement des systèmes interconnectés et des systèmes de distribution de flux en réseaux (distribution d'énergie, de fluides, de produits, d'information mais aussi collecte de déchets, d'eaux usées..). Ces recherches nécessitent de résoudre des problèmes de modélisation de système pour lesquels la fonction de structure est variable en fonction de l'environnement et des objectifs assignés au système.

Ce projet de recherche s'intègre naturellement dans le département Contrôle - Identification

- Diagnostic (CID) et dans le département Ingénierie des Systèmes Eco-Techniques (ISET) du Centre de Recherche en Automatique de Nancy (CRAN). Il s'inscrit dans le projet : « Co-conception de systèmes dynamiques sûrs de fonctionnement » (CSDF-CID) ; et le projet : « Sûreté de Fonctionnement Système » (SdFS- ISET) et éventuellement à moyen terme dans un nouveau projet focalisé sur l'intégration dans la commande des systèmes dynamiques, de connaissances liées à l'environnement économique, social et naturel avec l'idée principale de maîtriser l'impact du système sur son environnement en garantissant sa rentabilité et sa pérennité.

1 Les axes de mon projet de recherche

1.1 Introduction

Mes activités de recherche et l'expérience acquise durant l'encadrement des thèses, m'ont permis d'acquérir une démarche structurée et une expertise dans la formalisation de modèles graphiques probabilistes dans le domaine de la sûreté de fonctionnement. Elles constituent un socle de connaissances qui me sert de support :

- pour élargir le champ d'application des modèles graphiques probabilistes ;
- pour identifier les limites des formalismes de modélisation graphiques probabilistes actuellement disponibles ;
- pour envisager l'exploitation de nouveaux formalismes de modélisation graphiques probabilistes ;
- pour formaliser de nouvelles méthodologies de construction de modèles graphiques probabilistes.

C'est à partir de ces connaissances que s'oriente mon projet de recherche qui nécessite de faire évoluer mes activités de recherche vers de nouveaux formalismes de modélisation et de nouvelles méthodes de formalisation des modèles pour répondre à des problèmes qui ne trouvent pas encore de solution aujourd'hui.

De nouvelles pistes sont en cours de développement dans les communautés scientifiques des mathématiques et de l'informatique tels que le formalisme de modèle graphique relationnel PRM (Getoor et al. 2007 ; Wuillemin et Torti 2012 ; Chulyadyo et Leray 2014) ou tels que les algorithmes d'inférences dans les modèles graphiques probabilistes dynamiques (Manfredotti 2009 ; Koller 2009 ch. 15 pp 651-691 ; Russel et Norvig 2010 pp 590-606 ; Bouillaut 2014). Les PRM dynamiques (Manfredotti 2009) commencent à être exploités mais ils restent en cours de développement. Ces nouveaux formalismes doivent être étudiés pour en maîtriser le potentiel et les limites. Nous proposons de suivre l'évolution et les nouvelles adaptations de ces outils de modélisation pour répondre à des problèmes concrets et complexes. Ces nouvelles avancées dans la modélisation probabiliste sont donc à exploiter pour résoudre les problèmes d'analyse de risque ou de sûreté de fonctionnement et de commande de système. Les évolutions des méthodes de modélisation devraient permettre :

- La synthèse de modèles probabilistes de très grande taille ne pouvant plus être réalisée à la main ; nécessitant la formalisation de méthodes de construction de ces modèles.

- L'inférence dans des modèles probabilistes de dimension variable et de structure variable ce qui permet d'étendre les analyses de sûreté de fonctionnement à des nouvelles classes de systèmes plus complexes. Cela nécessite des travaux de recherche sur la formalisation générique des modèles de ces nouvelles classes de systèmes.
- La propagation des incertitudes épistémiques (liées au manque de connaissance) et la modélisation de mondes ouverts (pas de connaissance exhaustive des évènements), ce qui nous donne des possibilités d'intégration, dans le champ des connaissances modélisées, de dimensions partiellement connues mais critiques (comme les réactions humaines). Cela conduit à un travail de recherche sur la formalisation de ces connaissances et la définition de leurs interactions avec le reste du modèle.
- Enfin l'exploitation de la dimension temporelle ou dynamique pour fusionner des processus probabilistes dynamiques non indépendants, ce qui nous permet des calculs de plus en plus rapides sur des processus réactualisés en fonction d'un environnement en évolution permanente et d'envisager des projections dans le futur, c'est à dire, le pronostic de fonctionnement ou de dysfonctionnement d'un système.

Mon projet de recherche est d'exploiter ces nouvelles capacités de calculs et de modélisation afin de résoudre des problèmes concrets se déclinant en trois axes que nous présentons dans les sections suivantes :

- l'intégration de connaissances probabilistes dans la stratégie de commande des systèmes dynamiques ;
- la modélisation probabiliste en maîtrise des risques des systèmes sociotechniques et leurs impacts sur le développement durable ;
- la formalisation de modèles graphiques probabilistes en sûreté de fonctionnement pour de nouvelles classes de systèmes.

1.2 L'intégration de connaissances probabilistes dans la stratégie de commande des systèmes dynamiques

Mes activités de recherche s'orientent vers l'analyse de la commande et de la sûreté de fonctionnement des systèmes de distribution de flux en réseaux. Ces flux peuvent être des flux d'information, des flux d'énergie, par exemple électrique ou calorifique, ou des flux de matières telles que de l'eau, du pétrole, du gaz. La gestion des systèmes de distribution de flux en réseaux est un problème de commande ouvert car :

- Ils sont multi-entrées car ils sont approvisionnés par des ressources multiples.
- Ils sont multi-sorties car ils répondent à plusieurs demandes indépendantes des consommateurs.
- Ils ont une structure compliquée car ils sont constitués d'un grand nombre de composants avec des redondances matérielles ou fonctionnelles.
- Ils sont complexes car une partie du système peut contribuer à plusieurs objectifs.
- Ils peuvent être critiques et nécessiter de respecter des contraintes de sûreté de fonctionnement importantes.

Les techniques de commande optimale apportent des solutions intéressantes de gestion intelligente des réseaux de distribution (Cembrano et al. 2000 ; Hug-Glanzmann et Andersson, 2009 ; Pascual et al. 2013). Pour les systèmes sur-actionnés des méthodes d'allocations de commandes permettent de distribuer les objectifs sur les actionneurs (Johansen et Fossen, 2013). Malheureusement les algorithmes de commandes prennent rarement en compte la durée de la mission et n'optimisent pas la commande pour garantir le maintien des objectifs tel que la disponibilité du flux sur la durée restante de la mission.

Notre objectif est d'intégrer la fiabilité des actionneurs dans la synthèse de commande de manière à garantir une plus grande disponibilité du système à la fois dans le fonctionnement nominal et en présence de défauts (dérives) ou de défaillances (pannes) d'actionneurs. Toutefois, cette allocation de commande nécessite un modèle permettant d'évaluer la capacité à atteindre les objectifs en fonction de la dégradation fonctionnelle ou matérielle des composants au cours de leur mission. Nous orientons donc nos recherches vers le problème de l'intégration du pronostic dans la synthèse de la commande du système alors que le pronostic est classiquement appliqué à l'évaluation de date d'intervention de maintenance. Cette notion de pronostic est donc à étendre dans ce nouveau contexte caractérisé pas un environnement variable sur un horizon de mission borné.

Dans le cadre de la commande des systèmes tolérants aux défauts et aux défaillances, l'intégration de modèles de fiabilité dans la synthèse de la loi de commande des systèmes nécessite une modélisation dynamique de la fiabilité. Le calcul de la fiabilité et de la disponibilité doit tenir compte du vieillissement des composants en lien avec leurs sollicitations. Notre objectif est de prendre en compte ces informations en cours de fonctionnement pour élaborer une commande réactive aux changements en ligne des caractéristiques de fiabilité des composants. Comme nous l'avons montré dans nos recherches, les RBD fournissent un formalisme de modélisation de la fiabilité intégrant des observations sur l'environnement et les contraintes supportées par les composants, notamment la modélisation IOHMM.

La modélisation dynamique de la fiabilité du système devient complexe dès que l'on considère un système multicomposant car le modèle intègre alors plusieurs HMM (Le et al. 2014). Le problème augmente encore en complexité lors de l'intégration des contraintes d'exploitation et des perturbations dues à l'environnement, par exemple en utilisant des IOHMM. Dans cette situation l'inférence dans le modèle probabiliste est difficile car, lors d'une exploitation en ligne, les processus de dégradation des composants ne peuvent pas être considérés comme indépendants ; ils sont liés par les observations de l'état du système et de l'environnement.

Dans cette problématique de commande, le MGP est exploité pour fournir une estimation (pronostic) sur le temps de mission restant de la fiabilité des composants et du système. Cette estimation doit être intégrée dans la synthèse des commandes pour définir une loi de commande préservant l'intégrité et les performances du système. Des recherches sont nécessaires sur les algorithmes de commande existants afin de définir s'ils peuvent intégrer dans la phase d'optimisation des calculs issus d'un MGP dynamique. A plus long terme les recherches porteront sur les évolutions des algorithmes de commande intégrant des MGP.

Enfin pour prouver l'efficacité de ces nouvelles méthodes de commande des systèmes permettant d'intégrer des pronostics probabilistes sur des caractéristiques de sûreté de fonctionnement, il est nécessaire d'évaluer le gain de fiabilité du système. Cette analyse est à développer, les solutions envisagées reposent sur des techniques de simulations balayant les scénarios de défaillance et de reconfiguration du système de commande.

1.3 La modélisation probabiliste en maîtrise des risques des systèmes sociotechniques et leurs impacts sur le développement durable

Dans la problématique globale de maîtrise des risques, les entreprises doivent faire face à des changements réglementaires qui les incitent à traiter plusieurs risques conjointement comme le préconise les différentes directives du ministère de l'écologie, du développement durable et de l'énergie. Selon la direction générale de la prévention des risques, la mise en œuvre des politiques de précaution, de prévention et de protection repose sur quartes points :

- « La réduction des risques à la source, via la substitution de substances toxiques ou cancérigènes par des produits moins dangereux ou la mise en œuvre de procédés intrinsèquement moins dangereux et en recourant au principe des meilleures techniques disponibles. »
- « La limitation de l'exposition au risque résiduel, notamment en maîtrisant l'urbanisation dans les zones à risques ou grâce à des ouvrages de protection contre les risques naturels. »
- « La prévention au quotidien, à travers une attention portée aux questions liées à l'exploitation et à la maintenance et aux facteurs techniques, organisationnels et humains. »
- « Une vigilance et une alerte permanentes permettent d'anticiper toute dérive, de prévoir la survenue d'événements naturels et d'identifier les signaux faibles en termes de risques chroniques. »

Nos travaux de recherche contribuent plus particulièrement au point trois. L'environnement physique et réglementaire influence fortement les différents enjeux d'un système sociotechnique tel que la disponibilité, la sûreté, le maintien du patrimoine dans la durée en limitant les impacts sur l'environnement. La maîtrise des risques implique alors de modéliser dans une même vue :

- les risques affectant le système technique ; leur probabilité d'occurrence et la gravité de leurs conséquences sur les enjeux du système étudié ;
- les influences de l'environnement physique et réglementaire sur l'occurrence des risques techniques ;
- l'impact potentiel des actions humaines de maintenance et de conduite sur la défaillance des composants du système, et leurs impacts sur les enjeux mentionnés précédemment ;
- L'analyse des actions humaines dans leur contexte organisationnel.

Cette vue globale des risques en lien fort avec l'environnement physique et réglementaire permet de prioriser les risques en fonction de leurs impacts multiples.

Dans ce contexte évolutif de la gestion des risques industriels, mes perspectives sont de

développer une approche qui vise à traiter, à moyen terme, des systèmes complexes soumis à des risques de natures différentes intégrant le comportement humain qui peut s'écarter des procédures dans certaines conditions d'incidents ou d'accidents. L'enjeu est de savoir traiter des systèmes sociotechniques pris dans leur environnement physique et réglementaire en y intégrant les erreurs humaines ainsi que le phénomène de résilience humaine.

Puis à plus long terme, mes perspectives sont de développer l'intégration des enjeux du développement durable (sociale, économique et environnementale), dans les variables du modèle du système sociotechnique. L'objectif est de contribue à une meilleure maîtrise des systèmes en accord avec les principes de développement durable. Dans une approche de modélisation probabilistes, il est possible de développer des modèles d'estimations des retombées sur les enjeux du développement durable et de les relier aux actions et décisions envisagées. Cette modélisation permet l'évaluation de solutions durable en maîtrise des risques, mais elle nécessite de définir des variables caractéristique de l'impacte positif et négatif des solutions sur les enjeux du développement durable.

Pour prendre en compte l'incertitude dans ce type de modèle nous proposons d'exploiter des modèles probabilistes. Le problème de l'incertain épistémique met en questionnement la théorie des probabilités reposant sur des hypothèses exhaustives et disjointes. De plus, dans le cas précis de la sûreté de fonctionnement, les données sont bien souvent incomplètes et en faibles quantités. Pour résoudre ce problème, nos recherches s'orientent sur la modélisation par les Réseaux de Fonction de Croyance (RFC) qui permettent de propager des intervalles de probabilités. Nous avons fait le lien entre les algorithmes d'inférence des RB et la théorie de Dempster-Shafer. Nous avons proposé un cadre de modélisation des Réseaux de Fonction de Croyance (RFC) reposant sur une généralisation du cadre d'application des algorithmes d'inférence de RB. Ces travaux ouvrent le champ d'application des RFC, qui n'était jusqu'alors pas envisageable par manque d'outils de modélisation. Cette technique de modélisation devrait prendre tout son sens dans son application à la modélisation de la résilience humaine et l'estimation des impactes sur les enjeux du développement durable.

Dans notre cadre d'application, la dimension des modèles nécessite le développement de modèles de réseaux de fonctions de croyances sur le principe de la logique du premier ordre telle que les PRM. Nous proposons de définir un nouveau formalisme de modélisation par généralisation des PRM à la Théorie de Dempster-Shafer. Les perspectives dans ce domaine sont la formalisation de Modèles Relationnels de Fonctions de Croyances par généralisation des PRM.

Enfin l'intégration de la notion dynamique (temporelle) pour décrire les scénarios sous la forme de séquences d'évènements conduisant à des situations critiques devrait pouvoir être pris en compte sous la forme de modèles probabilistes dynamiques. Notre perspective dans ce domaine est de formaliser un modèle de risque et d'en assurer le calcul par des méthodes probabilistes efficaces comme les PRM dynamiques. Les fondements théoriques existent mais il n'existe aucun outil logiciel à ce jour permettant de formaliser ce type de modèle. Notre travail de recherche est de développer des méthodologies de construction de modèle PRM et de RFC étendue en suivant les développements des formalismes de modélisation et

des algorithmes d'inférence.

1.4 La formalisation de modèles graphiques probabilistes en sûreté de fonctionnement pour de nouvelles classes de systèmes

Les réseaux bayésiens sont des modèles graphiques probabilistes considérés comme un formalisme mathématique solide, supportés par des plateformes logicielles de simulation performantes. L'apparition d'outils ergonomiques pour la modélisation et le calcul probabiliste permet l'exploitation des réseaux bayésiens par une large communauté académique mais aussi industrielle, favorisant un large éventail d'utilisations dans l'analyse de risque, l'évaluation de la fiabilité, le diagnostic de défaillance, le pronostic de maintenance, etc. Ce formalisme mathématique reçoit aujourd'hui la reconnaissance de la communauté scientifique internationale.

Les recherches sont nombreuses sur le développement d'algorithmes de calcul dans des réseaux probabilistes de taille de plus en plus grande, intégrant des variables temporelles, continues (Russel et Norvig 2010 ; Koller 2009). Nous n'avons pas pour objectif de travailler sur ces algorithmes. Notre objectif est de contribuer à la méthodologie de construction des modèles répondant à des problèmes d'analyse et d'estimation dans notre champ d'expertise, c'est-à-dire, la sûreté de fonctionnement et la maîtrise des risques.

Les systèmes de distribution de flux en réseaux sont intéressants du point de vue de la fiabilité. Pour pouvoir développer ce nouveau champ d'application mes activités de recherche sur la modélisation multi-état doivent être étendues pour évaluer (pronostiquer) sous une formulation probabiliste la satisfaction de contraintes, d'objectifs ou de performances d'un système de distribution de flux en réseaux. Dans un système de distribution de flux en réseaux la fonction de structure fiabiliste du système peut changer en fonction de la demande des consommateurs et des capacités des composants du système. Par exemple des composants en redondance active (en parallèle) pour une charge nominale d'un systèmes de distribution de flux en réseaux peuvent être considérés en série du point de vue de la fiabilité à cause d'une demande trop importante conduisant à la saturation d'une partie des composants. Ce phénomène peut aussi apparaître :

- à l'issue d'une perte d'efficacité d'un composant par exemple à cause d'une dégradation de son état ou l'apparition d'un défaut,
- ou lors de la prise en compte de plusieurs demandes indépendantes sur les systèmes de distribution de flux.

La modélisation de la fiabilité multi-état par RB est une direction de recherche que je souhaite faire évoluer pour résoudre ce problème.

Au regard de la taille des systèmes de distribution de flux en réseaux, les modèles RB seront compliqués en plus d'être complexes. Le formalisme de modélisation par PRM est l'orientation à développer dans cet axe de recherche. En effet, les PRM permettent d'envisager la manipulation de modèles avec plus d'un millier de variables c'est à dire une échelle en cohérence avec la problématique de modélisation des systèmes de distribution de flux en réseaux. Un PRM est instancié en fonction de la requête de calcul, il devrait offrir la capacité d'adaptation dynamique nécessaire à la modélisation de la fiabilité en ligne pour la commande intégrant des connaissances fiabilistes.

Aujourd'hui les systèmes considérés en sûreté de fonctionnement et en maîtrise des risques sont constitués de plusieurs centaines de composants. Il est donc nécessaire de travailler sur des outils de génération automatique de modèles à partir de la représentation graphique de la description du système classiquement utilisée par les industriels. Les Modèles PRM reposent sur un langage textuel de description du modèle. Ce langage est intéressant car il permet une conversion automatique en texte des informations nécessaires à la construction de modèle.

En sûreté de fonctionnement, les modèles que nous construisons reposent bien souvent sur des modèles hiérarchiques cependant, dans un système complexe, les fonctions sont réalisées pas plusieurs composants et les composants réalisent eux aussi plusieurs fonctions qui peuvent être utilisées à des niveaux très différents. Dans ce cas, une représentation hiérarchique sous la forme d'un arbre n'est pas appropriée pour décrire ce type de système. Un réseau bayésien ne nécessite pas une structure hiérarchique, car il repose sur un graphe orienté sans circuit et correspond bien à ce type de structure. Je souhaite continuer à développer des méthodes de modélisation qui permettent d'exploiter, en plus de la manipulation des variables multi-états, cette capacité de modélisation de RB.

Des travaux de recherche font le lien entre des représentations basées sur le langage SysML (Systems Modeling Language) et la représentation AMDE (David et al. 2008), ou le langage AltaRica (David et al. 2010). Mais il n'existe pas encore de travaux reliant SysML au langage de description des PRM. Je souhaite développer cette activité de recherche pour tirer avantage d'une description des systèmes dans un formalisme connu des industriels reposant sur l'ingénierie système sans aucune restriction du langage et formaliser des modèles multi-états tirant tous les avantages du formalisme PRM.

2 Collaborations supports de mon projet de recherche

Pour me permettre de développer ce projet de recherche une partie des moyens nécessaires repose sur les relations que nous pouvons établir entre plusieurs laboratoires pour répondre à des appels d'offre ou pour déposer des projets de recherche nationaux (ANR) ou internationaux (Projet Européen) ou l'encadrement de thèses en cotutelle. Durant mes activités de recherche, des contacts et des collaborations se sont établis avec des collègues français ou étrangers. Mon projet repose sur ces contacts et nécessite de les développer.

2.1 Collaborations en relation avec l'axe : intégration de connaissances probabilistes dans la stratégie de commande des systèmes dynamiques

- Universitat Politècnica de Catalunya (UPC), Pr. Vince Puig, Fatiha Nejjari et Ramon Sarrate Estruch, Espagne ;
  Vicenc Puig Cayuela, et ses collègues travaillent sur la commande tolérante de systèmes complexes. Ils se sont récemment orientés vers l'intégration et l'analyse de la fiabilité de ces systèmes. Le Pr. Vicenc Puig Cayuela est venu au CRAN pour une durée de 2 mois en 2012, puis Jean Carlo Salazar Cortes (doctorant) est venu 4 mois en 2014 puis 4 mois en 2015. Ces différents séjours ont permis de démarrer une collaboration entre nos équipes (2 publications communes plus 2 en soumission). Jean Carlo Salazar Cortes viendra pour 1 séjours scientifiques de 4 mois au CRAN en

2016. Cette collaboration permet de couvrir une application sur un système de distribution de flux en réseau. Je souhaite renforcer cette collaboration avec les chercheurs Vicenc Puig Cayuela, Fatiha Nejjari et Ramon Sarrate Estruch ainsi que mes collègues du CRAN Didier Theilliol et Christophe Simon. Nous avons comme objectif de démarrer une thèse en cotutelle entre l'Université de Barcelone et l'Université de Lorraine.
Bilan : Une thèse en cotutelle en 2016-2019.

- Laboratoire Gipsa-Lab : Pr. Christophe Bérenguer ; Pr. Jean-Marc Thiriet
  Christophe Bérenger développe des méthodes de prédiction de défaillance dans le cadre de la maintenance prédictive et le pronostic de défaillance. Ses recherches s'orientent vers des estimations en lignes, ce qui conduit aux mêmes problèmes que je rencontre dans l'évaluation des commandes intégrant la fiabilité des systèmes. Les modèles que nous utilisons sont très proches, et nos approches sont complémentaires car l'une est orientée vers la maintenance et l'autre vers la commande, toutes deux afin de garantir la disponibilité du système jusqu'au moment de l'intervention de maintenance. Cette collaboration est intéressante pour le développement de l'axe commande de système reconfigurable et intégration des connaissances probabilistes. De plus, Jean Marc Thiriet a travaillé sur la prédiction de la dégradation des moyens de contrôle et des objectifs d'un système. Ces dégradations sont liées au réseau de communication, au système et à son environnement. La modélisation par RBD est utilisée pour ce pronostic. Jean-Marc est membre du GTR de l'IMDR que j'anime. Ces travaux sont complémentaires à la problématique de commande intégrant les modèles de fiabilité que je développe. Je souhaite donc relancer des collaborations avec le Gipsa-Lab sur ces thématiques communes.

- Laboratoire GSCOP : Dr. Hdr. Eric Zamaï ;
  Eric Zamaï propose dans ses recherches une méthodologie permettant d'améliorer la maîtrise des risques dans le domaine particulier des ateliers de fabrication des circuits intégrés. Ses recherches se focalisent sur la problématique des défaillances mais aussi les dérives de fonctionnement des équipements. Les solutions envisagées reposent sur une approche probabiliste de modélisation par réseaux Bayésiens. Ses recherches sont très proches de mes objectifs et nous devrions pouvoir démarrer des collaborations en lien avec l'axe commande de système reconfigurable et intégration des connaissances probabilistes.

  Cet axe de recherche étant prioritaire pour mon projet de recherche à court terme, je déposerai **une demande de financement de thèse au CRAN (2017-2020)** pour nous permettre de conserver notre position de leader sur cette thématique de recherche.

2.2 Collaborations en relation avec l'axe : modélisation probabiliste en maîtrise des risques des systèmes sociotechniques

- EDF, département de Maîtrise des Risques Industriels (MRI), Carole Duval ; Pierre Lebot ; Emmanuel Serdet et Aurélie Leger ;
  Je souhaite poursuivre l'application de mes travaux en maîtrise des risques appliqués

aux systèmes de production d'énergie électrique, principalement dans le secteur nucléaire en lien avec le département de Maîtrise des Risques Industriels (MRI) de EDF. Je souhaite donc pérenniser mes travaux avec Carole Duval, Pierre Lebot, Emmanuel Serdet et Aurélie Leger. Nous sommes en cours de développement de recherches sur l'intégration de la dimension fiabilité humaine dans la modélisation AiDR. Nous avons une thèse CIFRE en cours. A plus long terme, ces travaux peuvent être appliqués à d'autres industries à risques. Mon objectif est de pouvoir en promouvoir l'application le plus largement possible notamment dans le secteur des industries à risques pour que ce travail permette de mieux maîtriser ces activités industrielles ayant potentiellement des impacts forts sur notre société et notre environnement.
Bilan : Une thèse CIFRE EDF-CRAN 2013-2016.

- IRSTEA (Grenoble, Aix en Provence), Tacnet Jean-Marc ;
  Jean-Marc Tacnet travaille sur l'évaluation de l'efficacité des ouvrages de protection pour des risques naturels (éboulements ; coulées de boue ; inondations). Ces travaux s'inscrivent dans une démarche de maîtrise des risques intégrant la résilience du système subissant l'occurrence des évènements naturels. Les incertitudes en cause nous conduisent à envisager une résolution du problème par une modélisation par réseaux de fonctions de croyances. Nous travaillons conjointement Christophe Simon, Benoit Iung et moi-même sur la formalisation d'un projet H2020.
  Bilan : une thèse associée au projet Européen 2017-2020

- Université de Western Ontario, Pr. Jin Jiang, Canada ;
  Notre savoir-faire en analyse de risque et en modélisation probabiliste dans le domaine nucléaire est complémentaire aux travaux de recherche de Jin Jiang. Nous avons déjà évoqué ensemble le développement d'une méthode de pilotage sûre expérimentée sur le simulateur de l'Université de Western Ontario. Cette collaboration n'est pas encore effective, elle pourrait être développée dans les années à venir. Ceci permettrait d'exporter notre savoir faire.

2.3 Collaborations en relation avec l'axe : formalisation de modèles graphiques probabilistes en sûreté de fonctionnement

- Universita' del Piemonte Orientale, Pr. Luigi Portinale, Italie ;
  Luigi Portinal travaille depuis de longues années sur la modélisation par RBD et principalement dans la poursuite des travaux de Andrea Bobbio qui ont pour objet d'établir des conversions entre arbres de défaillances dynamiques et RBD. Nos visions sont complémentaires. D'un coté une approche focalisée sur un langage de modélisation existant et reconnu mais avec les restrictions inhérentes à ce langage et de notre côté une modélisation multi-état reposant sur la transcription de connaissances fonctionnelles et dysfonctionnelles. Nous devons développer nos relations pour pouvoir être capables de déposer des projets européens. Nous organisons conjointement une session spéciale sur l'application des MGP à la sûreté de fonctionnement au diagnostic et au pronostic.

- IFSTAR, MdC HDR Laurent Bouillaut ;

Laurent Bouillaut travaille sur les problèmes de sûreté de fonctionnement et de maintenance des infrastructures ferroviaires. Il est spécialiste de la modélisation par réseaux bayésiens dynamiques, ses recherches portent sur les algorithmes d'inférence et la modélisation pour l'optimisation de la maintenance. Nos travaux sont complémentaires. Nous avons travaillé ensemble lors du poste d'ATER de Laurent qui était à l'ESSTIN, puis pour l'encadrement de la thèse, en cotutelle entre l'INRETS et le CRAN, de Abdeljabbar Ben Salem. Nous pourrions mettre en place des collaborations enrichissantes en relation avec les algorithmes d'inférence des MGP dynamique.

- Laboratoire d'Informatique de Nantes Atlantique : Pr. Philippe Leray ;
  Philippe Leray développe actuellement des recherches sur la modélisation par graphes probabilistes, son activité s'est focalisée récemment sur les modèles PRM. Nous avons abordé au CRAN les PRM dans la thèse de Gabriella Medina, et aujourd'hui il nous semble inévitable de développer cet axe de recherche pour véritablement répondre aux problèmes de maîtrise des risques posés par les industriels. Les travaux de Philippe Leray se positionnent de façon complémentaire à nos travaux. Philippe Leray a le savoir faire sur les outils et les algorithmes d'apprentissage et d'inférence dans les modèles probabilistes.

- Laboratoire PRISME, Pr. Frederique Kratz et MdC Vincent Idasiak ;
  Frédérique Kratz et Vincent Idasiak travaillent sur la modélisation SysML appliquée à la sûreté de fonctionnement notamment pour la génération automatique de tableaux AMDE et la génération de modèle AltaRica. Je pence que nous pouvons développer des relations pour contribuer à la formalisation de modèle PRM reposant sur des descriptions de systèmes industriels en langage SysML. Ce travail intègre naturellement mes collègues du CRAN Eric Levrat, Benoit Iung et Jean François Pétin qui sont eux aussi spécialistes de cet axe de recherche.

3 Projet de rayonnement scientifique

3.1 Proposition d'animation scientifique locale

La recherche n'est pas un travail individuel et après toutes ces années, je suis persuadé que l'innovation ne peut naître que de la confrontation de différents points de vues. Durant ces années passées au CRAN, j'ai eu le plaisir de travailler avec un ensemble de chercheurs, comme l'illustre la répartition des co-auteurs sur mes publications internationales (Figure 47).

Ces chercheurs : D. Theilliol, B. Iung, C. Simon, E. Levrat, D. Sauter, C Aubrun, JC Ponsart et F. Bicking contribuent avec des techniques et des méthodes différentes aux problèmes de modélisation en sûreté de fonctionnement, de maîtrise des risques et de commande des systèmes tolérants aux défauts et aux défaillances.

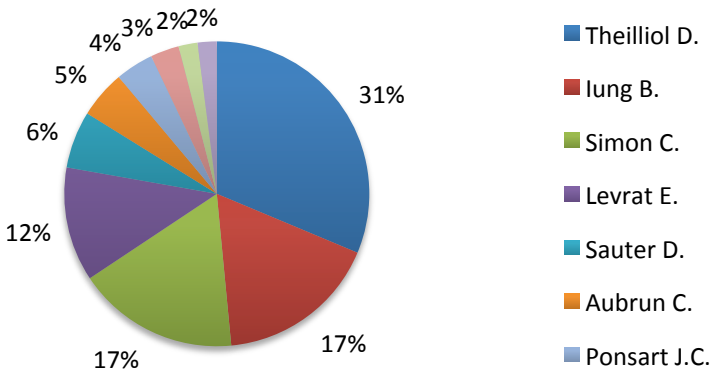


Figure 47 : Répartition des co-auteurs sur mes publications internationales

Un ensemble de chercheurs du CRAN avec qui je n'ai pas encore publié travaille sur des axes connexes ou complémentaires :

- Phuc DO VAN, qui maîtrise la modélisation des dégradations des composants. Ses recherches appliquées au pronostic pourraient être transposées à l'estimation de l'impact des charges de commande sur la fiabilité des composants avec notamment des approches par simulation.

- Samir ABERKANE, qui travaille sur des approches de commande intégrant des évènements de défaillance modélisés par des Chaines de Markov. Ses objectifs d'analyse de stabilité et de performance des systèmes sont des clefs pour garantir l'efficacité de ce type de commande.

- Samia MAZA, qui utilise des méthodes pour modéliser la fiabilité des systèmes de diagnostic ou la fiabilité de système tolérant aux défaillances. C'est une action de recherche nécessaire pour comparer l'apport de méthodes de commande des systèmes intégrant la fiabilité.

En terme d'animation scientifique locale, je suis prêt à m'investir dans l'organisation de temps d'échange et de travail avec pour objectif de fédérer ces recherches et de faire émerger un groupe de chercheurs autour d'un projet de recherche qui ne peut évidement pas être restreint à mon projet de recherche. Ce projet pourrait avoir pour objectif de contribuer à une plus grande maîtrise de la durabilité des systèmes par l'intégration dans une boucle d'optimisation des caractéristiques en liens avec la sûreté et la dégradation des composants. Les contributions pourraient porter sur des solutions permettant de garantir un fonctionnement sûr et durable sur la durée de la mission et/ou la durée de vie du système.

3.2 Projet d'animation scientifique nationale

Un de mes projets est de promouvoir la modélisation par RB dans les milieux industriels. Pour cela il est nécessaire de faire apparaître cet outil dans les normes sur lesquelles les industriels se basent pour leur travail. Nous avons franchi une première étape en publiant des articles dans la bibliothèque de l'AFNOR sur l'application des RB à la SDF. J'espère, sur le plus long terme, que mes relations avec les industriels, mon activité à l'IMdR notamment

comme animateur du Groupe de Travail et de Réflexion (GTR) de l'IMdR : Réseaux probabilistes appliqués à la Maîtrise des Risques et à la Sûreté de Fonctionnement et les journées thématiques que nous organisons me permettront d'être référencé comme expert en RB et me donneront l'opportunité d'impulser un travail de mise à jour des outils de modélisation adossé aux normes de sûreté de fonctionnement.

Enfin j'ai pour projet de croiser le GTR-IMdR et le GT S3 du GDR-MACS. Cela pourrait être à l'occasion d'une journée thématique organisée conjointement sur la modélisation graphique probabiliste appliquée à des systèmes complexes en sûreté de fonctionnement, en commande et en diagnostic des systèmes dynamiques.

3.3 Projet d'animation scientifique internationale

Pour pouvoir promouvoir l'application des outils de modélisation tels que les réseaux bayésiens et les PRM en sûreté de fonctionnement, il est important de prendre des responsabilités dans des réseaux internationaux. Ces méthodes de modélisation sont de plus en plus utilisées, et il est nécessaire de tisser un réseau de relations avec les spécialistes internationaux : sur la partie modélisation graphique probabiliste je suis en relation avec Luigi Portinale et Martin Neil ; sur la partie sûreté de fonctionnement je suis en relation avec Christophe Bérenguer, Jin Jiang, et Enrico Zio, et enfin sur la partie commande de système tolérant aux défauts je suis en relation avec Youming Zhang, Vicenc Puig Cayuela et Vincent Cocquempot.

J'ai pour objectif de m'investir et de prendre des responsabilités à un niveau international dans les comités techniques d'évaluation de l'IFAC ou IEEE. Une première étape est de proposer un groupe de travail (Working group) dans le TC 6.4. Fault Detection, Supervision & Safety of Technical Processes-SAFEPROCESS, sur la problématique de la modélisation graphique probabiliste appliquée au diagnostic, à la commande tolérante aux défaut et à la sûreté de fonctionnement, dans la continuité de la session invitée que je propose avec Luigi Portinal au Safeprocess 2015.

Mes activités d'expertises pour les revues me permettent d'être en contact avec les éditeurs de revues scientifiques internationales. Je suis prêt à m'investir dans le comité d'édition (Editorial Board) des revues du domaine : en sûreté de fonctionnement, maîtrise des risques et plus particulièrement sur la thématique de la modélisation graphique probabiliste. Les revues qui publient régulièrement des articles dans ce domaine sont Reliability Engineering & System Safety et Engineering Applications of Artificial Intelligence.

5 Conclusion (20 ans en 20 lignes)

Dès le début de mon parcours universitaire, j'étais passionné par l'intelligence artificielle. Mes livres de chevet portaient sur la compréhension du langage naturel et les systèmes experts. Puis j'ai eu la chance en 1994 de pouvoir poursuivre mes études en master avec l'objectif de devenir enseignant chercheur.

J'ai commencé mes travaux de recherche en diagnostic de défauts au CRAN avec Didier Theilliol et Dominique Sauter. L'objectif était d'intégrer des connaissances autres que celles du modèle du système et ses résidus et ajouter de l'expertise par un système expert. Puis j'ai

poursuivi avec un doctorat dirigé par Sylviane Gentil (Gipsa-LAG) reconnue pour son travail d'intégration de l'intelligence artificielle en automatique. Ce travail de thèse m'a conduit à des recherches en identification paramétrique appliquée au diagnostic de défauts.

J'ai ensuite pris la direction qui m'a conduit à travailler sur le problème de l'aide à la décision en maintenance avec Benoit Iung et Eric Levrat et la modélisation pour l'évaluation de la sûreté de fonctionnement de systèmes complexes avec Christophe Simon. Je alors poursuivi mes activités de recherche en intégrant l'intelligence artificielle par l'exploitation de la modélisation par Réseaux Bayésiens.

Aujourd'hui, j'ai pour projet de revenir à l'intégration des connaissances de sûreté de fonctionnement dans les problématiques de commande et de diagnostic des systèmes continus. C'est un re-bouclage sur mes activités de recherche initiales avec finalement le même objectif, c'est-à-dire accroître l'efficacité de l'intelligence embarquée dans les systèmes pour leur donner une plus grande efficacité et durabilité.

Références bibliographiques

Allen D., Darwiche A. (2003). New advances in inference by recursive conditioning. In: Proceedings of UAI, 2-10.

Ansell J.I., Phillips M.J. (1994). Practical methods for reliability data analysis. Oxford University Press Inc. ISBN 0 19 853664 X.

Aven T. and U. Jensen (1999) Stochastic models in reliability. (Applications of mathematics), Springer-Verlag, ISBN 0-387-98633-2, SPIN 10695247, New York.

Bagdonavicius, V., Nikulin, M. "Estimation in Degradation Models with Explanatory variables", Lifetime Data Analysis, 7, 85-103, 2001.

Ben Salem A., Modèles Probabilistes de Séquences Temporelles et Fusion de Décisions. Application à la Classification de Défauts de Rails et à leur Maintenance. Thèse de doctorat de Nancy Université, 7 mars, (2008), (138 pages).

Ben Salem A., Muller A., Weber P., Dynamic Bayesian Networks in system reliability analysis. 6th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, Beijing, P.R. China (30/08/2006), pp. 481-486.

Ben Salem A., Bouillaut L., Aknin P., Weber P. (2004) Dynamic Bayesian Networks for classification of rail defects. IEEE 4th International Conference on Intelligent Systems Design and Applications, Budapest, Hungary, August 26-28.

Bengio Y., Markovian models for sequential data. *Neural Computing Surveys*, 2, pp 129-162, 1999.

Bensi M., A. Der Kiureghian, D. Straub, (2013) Efficient Bayesian network modeling of systems. Reliability Engineering & System Safety, Volume 112, April 2013, Pages 200-213.

Bicking F., Weber P., Theilliol D., Aubrun C. Control allocation using reliability measures for over-actuated systems. Dans Intelligent Systems in Technical and Medical Diagnostics (2014) 487-497

Bicking F., Weber P., Aubrun C., Theilliol D. Control allocation using reliability measures for over-actuated system. Dans 11th International Conference on Diagnostics of Processes and Systems, DPS 2013 - 11th International Conference on Diagnostics of Processes and Systems, DPS 2013, Pologne (2013a).

Bicking F., Weber P., Theilliol D. Reliability importance measures for fault tolerant control allocation. Dans 2nd International Conference on Control and Fault-Tolerant Systems, SysTol'13 - 2nd International Conference on Control and Fault-Tolerant Systems, SysTol'13, France (2013b).

Bobbio A., E. Ciancamerla, G. Franceschinis, R. Gaeta, M. Minichino and L. Portinale (2003). Sequential application of heterogeneous models for the safety analysis of a control system: a case study. Reliability Engineering and System Safety, 81 (3), September 2003, Pages 269-280.

Bobbio A., Portinale L., Minichino M., Ciancamerla E. (2001). Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. Reliability Engineering and System Safety. 71(3), 249-260.

Boudali H., Dugan J.B. (2005a). A new Bayesian network approach to solve dynamic fault trees. IEEE Reliability and Maintainability Symposium. 451-456, January 24-27.

Boudali H., Dugan J.B. (2005b). A discrete-time Bayesian network reliability modeling and analysis framework. Reliability Engineering and System Safety. 87(3), 337-349.

Boudali H., Dugan J.B. (2006). A continuous-time Bayesian network reliability modeling and analysis framework. IEEE Transaction on Reliability. 55(1), 86-97.

Bouillaut L., Weber P., Ben Salem A., Aknin P. Use of Causal Probabilistic Networks for the improvement of the Maintenance of Railway Infrastructure. IEEE International Conference on Systems, Man and Cybernetics, Hague, Netherlands, October 10-13, (2004).

Bouillaut L. (2014) Les modèles graphiques probabilistes : de la modélisation de la dégradation à l'optimisation de la maintenance de systèmes complexes. Habilitation à Diriger les Recherches, Université de Paris Est, octobre 2014.

Bouissou M. and J.L. Bon (2003). A new formalism that combines advantages of fault-trees and Markov models: Boolean logic driven Markov processes, Reliability Engineering and System Safety, 82 (2), pp 149-163.

Boutillier C., T. Dean, S. Hanks (1999). Decision-theoretic planning: structurel assumptions and computational leverage. Journal of Artificial Intelligence Research, 11, 1-94.

Boyen X. and Koller D. (1998) Tractable for Complex Stochastic Processes. Proceedings of the 14th Annual Conference on Uncertainty in AI (UAI), Madison, Wisconsin, July 1998, 33--42.

Celeux G., Corset F., Lannoy A., Ricard B. (2006) Designing a Bayesian network for preventive maintenance from expert opinions in a rapid and reliable delay. Reliability Engineering and System Safety. 91(7), 849-856.

Cembrano G., Wells G., Quevedo J., Pérez R., Argelaguet R., (2000) Optimal control of a water distribution network in a supervisory control system, Control Engineering Practice, Volume 8, Issue 10, October 2000, Pages 1177-1188, ISSN 0967-0661, http://dx.doi.org/10.1016/S0967-0661(00)00058-7.

Cocozza-Thivent C. (1997). Processus stochastiques et fiabilité des systèmes. Ed. Springer, Collection Mathématiques & Applications 28. ISBN 3-540-63390-1

Corazza M. (1975). Techniques mathématiques de la fiabilité prévisionnelle. Ed. Cepadues. Collection SUP'AERO. ISBN 2-85428-003-2

Cozman F. (2004) Axiomatizing Noisy-OR, 1-th European Conference on Artificial Intelligence (ECAI-04).

Cox, D.R. (1955) The analysis of non-markovian stochastic processes by the inclusion of supplementary variables. Proceedings of the Cambridge Philosophical Society, 51, 433-440.

Chulyadyo R., Leray P. (2014). A Personalized Recommender System from Probabilistic Relational Model and Users' Preferences. Procedia Computer Science 35, 1063-1072.

David, P. Idasiak, V. & Kratz, F. (2008). Towards a better interaction between design and dependability analysis: FMEA derived from UML/SysML models. Proceedings of ESREL 2008 and 17th SRA-EuropeAnnual Conference, Valencia, Spain.

David P., Idasiak V., Kratz F. (2010). Automating the synthesis of AltaRica Data-Flow models from SysML. Reliability, Risk and Safety: Theory and Applications – Briš, Guedes Soares & Martorell (eds), Taylor & Francis Group, London, ISBN 978-0-415-55509-8

De Rocquigny E. (2012) Modelling Under Risk and Uncertainty: An Introduction to Statistical, Phenomenological and Computational Methods. Wiley Eds, ISBN: 978-0-470-69514-2, 484 pages, April.

De Souza E., Ochoa P.M. (1992). *State space exploration in Markov models. Performance Evaluation Review. 20(1), 152-166.*

Department of Transport (1975) Health and Safety Executives: The Flixborough disaster – The court of Enquiry, US Department of Transport, 1975.

Doguc O., Ramirez-Marquez J.E. (2009) A generic method for estimating system reliability using Bayesian networks. Reliability Engineering & System Safety, Volume 94, Issue 2, February 2009, Pages 542-550.

Dugan J.B., Bavuso S.J., Boyd M.A. (1992). Dynamic fault-tree for fault-tolerant computer systems. IEEE Trans Reliab., 41(3), 363–377.

Duval C., Fallet-Fidry G., Iung B., Weber P., Levrat E., A Bayesian network-based integrated risk analysis approach for industrial systems: application to heat sink system and prospects development. Proceedings of the Institution of Mechanical Engineers, Part O : Journal of Risk and Reliability, 226(5):488–507, octobre (2012).

Duval C., Marle L., Paradowski V., Simon C., Weber P. Exemples d'application des réseaux Bayésiens. Dans BIVI Maîtrise des risques, (2014), 1-21

Fallet G. (2012). AiDR : Eléments pour l'amélioration de la robustesse et la propagation des incertitudes résiduelles. Thèse de doctorat de Nancy Université, 10 décembre (225 pages).

Fallet G., Duval C., Weber P., Simon C., Characterization and propagation of uncertainties in complex socio-technical system risk analyses. 1st international Workshop on the Theory of Belief Functions, Brest : France, (2010).

Fallet G., Duval C., Simon C., Weber P., Iung B., Expert judgments collecting and modeling: Application to the Integrated Risks Analysis (IRA) methodology. 3rd International Workshop on Dependable Control of Discrete Systems (DCDS), Saarbrucken : Deutschland, June, (2011), 72–77. DOI: 10.1109/DCDS.2011.5970321

Fallet G., Weber P., Simon C. Iung B., Duval C., Evidential network-based extension of Leaky Noisy-OR structure for supporting risks analyses. In 8th International Symposium SAFEPROCESS 2012, Mexique, august (2012).

Fallet-Fidry G., Duval C., Simon C., Levrat E., Weber P., Iung B. : Maîtrise et analyse des risques des systèmes intégrant les domaines techniques, humains, organisationnels et environnementaux. In Jean Arlat Nada Matta, Yves Vandenboomgaerde, éditeur : Supervision, surveillance et sûreté de fonctionnement des grands systèmes, Traité Information, Commande, Communication, IC2, 309–330. Hermès Science Publications, (2012).

Faÿ A., Jaray J.Y. (2000). A justication of local conditioning in Bayesian networks. International Journal of Approximate Reasoning 24(1), 59-81.

Flacke N., Margaria T., Floyd B., Duerr Specht M., Seemann Monteiro M., Halpern P., De Iaco F., Garcia Castrillo Riesgo L., Wazzan A., Weber P., Barletta C., Bellou A. (2014) Managing Knowledge in Emergency Care Technology. DGINA'14, German Society Interdisciplinary Emergency and Acute Medicine, 9th Annual Meeting 2014 (DGINA 2014) in Nuremberg on November 6th 2014.

Getoor L., Friedman N., Koller D., Pfeffer A., Taskar B., Probabilistic relational models, in: L. Getoor, B. Taskar (Eds.), An Introduction to Statistical Relational Learning, MIT Press, 2007, pp. 129–174.

Guenab F., (2007). Contribution aux systèmes tolérants aux défauts : Synthèse d'une méthode de reconfiguration et/ou de restructuration intégrant la fiabilité des composants. Thèse de doctorat de Nancy Université, 20 février, (150 pages).

Guenab F., Weber P., Theilliol D., Zhang Y.M., Optimal Design of Fault Tolerant Control System versus Reliability Analysis under Dynamic Behaviour Constraints. *International Journal of Systems Science*, **42**, 1, (2011), 219-233.

Guenab F., Theilliol D., Weber P., Zhang Y., Sauter D., Fault tolerant control system design: A reconfiguration strategy based on reliability analysis under dynamic behavior constraints. Session invitée, 6th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, Beijing, P.R. China (30/08/2006) pp. 1387-1392.

Guenab F., Theilliol D., Weber P., Ponsart J.C., Sauter D. Fault-tolerant control design based on cost and reliability analysis. 16th IFAC World Congress, Prague, Czech Republic, Juillet 4 – 8, (2005).

Guenab F., Join C., Ponsart J.C., Sauter D., Theilliol D., Weber P., A reliability approach to reconfiguration strategy: application to the IFATIS benchmark problem. Session invitee, 2nd IFAC Symposium on System Structure and Control. Oaxaca, Mexico, December 8-10, (2004a).

Guenab F., Theilliol D., Weber P., Ponsart J.C., Sauter D. Fault-tolerant control design based on cost and reliability analysis. Workshop on Advanced Control and Diagnosis (ACD), Karlsruhe, Germany, November 17 - 18, (2004b).Gertsbakh I. (2000). Reliability Theory : with applications to preventive maintenance. Ed. Springer. ISBN 3540-67275-3

Gonzales C., Wuillemin P.H. (2011). PRM inference using Jaffray & Faÿ's Local Conditioning. Theory and Decision. Springer. 71(1), 33-62.

Guyot B., et al. (2009). Validation et représentativité d'un Réseau Bayésien en analyse des risques et sûreté de fonctionnement. Projet IMdR P09-2.

Hug-Glanzmann G., Andersson G. (2009). Decentralized Optimal Power Flow Control for Overlapping Areas in Power Systems. IEEE Transaction on Power Systems, 24(1), February 2009.

Hung K. B., S. Venkatesk, G. West (1999). Layered dynamic probabilistic networks for spatio-temporal modelling. Intelligent Data Analysis, 3, 339-361.

Jaeger M. (2002), Relational Bayesian Networks: a Survey, Electronic Transactions on Artificial Intelligence, Linköping University Electronic Press, 6.

Jensen F.V. (1996). An Introduction to Bayesian Networks. UCL Press (Ed), London.

Jensen F.V., Lauritzen S., Olesen K. (1990). Bayesian updating in causal probabilistic networks by local computations. Computational Statistics Quarterly 4, 269-282.

Johansen TA., Fossen TI., (2013). Control allocation - A survey. Automatica, 49(5), May, pp 1087-1103, ISSN 0005-1098, http://dx.doi.org/10.1016/j.automatica.2013.01.035.

Kang C.W., Golay M.W. (1999). A Bayesian belief network-based advisory system for operational availability focused diagnosis of complex nuclear power systems. Expert Systems with Applications. 17, 21-32.

Kemeny J.G., (1979) Report of the President's Commission on The Accident at Three Miles Island.

Khakzada N., Khana F., Amyotte P. (2013). Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. Process Safety and Environmental Protection, 91, 46–53.

Khelassi A., (2011). Nouvelle méthodologie de synthèse de lois de commande active tolérante aux fautes garantissant la fiabilité du système. Thèse de doctorat de Nancy Université, 11 juillet (133 pages).

Khelassi A., Theilliol D., Weber P., (2011a). Reconfigurability Analysis for Reliable Fault-Tolerant Control Design, International Journal of Applied Mathematics and Computer Science (AMCS), 21, 3, 431-439.

Khelassi A., Theilliol D., Weber P., Zhang Y. (2012). Fault-tolerant compensation control incorporating actuator criticality. In 8th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, SAFEPROCESS 2012 , Mexico City, Mexique, août.

Khelassi A., Theilliol D., Weber P., D. Sauter. A novel active fault tolerant control design with respect to actuators reliability. 50th IEEE Conference on Decision and Control and European Control Conference, Orlando : Florida - USA, December 12-16 (2011b).

Khelassi A., Theilliol D., Weber P., Ponsart J.C. Fault-tolerant control design with respect to actuator health degradation: An LMI approach. IEEE Conference on Control Applications, Denver : Colorado - USA, September 28-30 (2011c).

Khelassi A., J. Jiang, Theilliol D., Weber P., Y. Zhang. Reconfiguration of Control Inputs for overactuated Systems based on Actuators health. 18th IFAC World Congress, Milan : Italy, August 29- September 02 (2011d).

Khelassi A., Weber P., Theilliol D., C. Aubrun. Evaluation of Fault Tolerant System against Actuators Aging applied to Flotation Circuit. 18th IFAC World Congress, Milan : Italy, August 29- September 02 (2011e).

Khelassi A., Weber P., Theilliol D., Reconfigurable Control Design for over-actuated Systems based on Reliability Indicators, Conference on Control and Fault-Tolerant Systems, Nice : France, October, (2010a), 365-370.

Khelassi A., Theilliol D., Weber P., Control Design for Overactuated Systems based on Reliability Indicators. UKACC International Conference on Control, Coventry : UK, September (2010b).Khelassi A., Theilliol D., Weber P., Reconfigurability analysis for reliable fault-tolerant control design. 7th Workshop on Advanced Control and Diagnosis, Zielona Gora : Poland, November (2009a).

Khelassi A., Theilliol D., Weber P., On reconfigurability for actuator faults under reliability constraints. IFAC Workshop on Automation in Mining, Mineral and Metal Processing, Vina del Mar : Chile, October (2009b).

Kjaerulff U. (1995). dHugin: a computational system for dynamic time-sliced Bayesian networks. Internationnal journal of forecasting, 11, 89-111.

Koller D. and Friedman N. (2009). Probabilistic graphical models : principles and techniques. Ed. Massachusetts Institute of Technology Press. ISBN 978-0-262-01319-2

Koller D. and Lerner U. (2000) Sampling in Factored Dynamic Systems. Invited contribution to the book Sequential Monte Carlo Methods in Practice, A. Doucet, J.F.G. de Freitas, and N. Gordon, Eds., Springer-Verlag, pp 470-490.

Koller D., Lerner U., Anguelov D. (1999). A General Algorithm for Approximate Inference and Its Application to Hybrid Bayes Nets. UAI 1999: 324-333.

Koller D. et Pfeffer A. (1998). Probabilistic frame-based systems. Proceedings of the 15th National Conference on Artificial Intelligence (AAAI), Madison, Wisconsin.

König, J., Nordstrom, L., Ekstedt, M. (2010). Probabilistic Relational Models for assessment of reliability of active distribution management systems. In: Probabilistic Methods Applied to Power Systems (PMAPS), 2010 IEEE 11th International Conference on, IEEE 454-459.

Langseth H. (2008). Bayesian Networks in Reliability: The Good, the Bad and the Ugly. Advances in Mathematical Modeling for Reliability. IOS Press. Amsterdam, Netherland.

Langseth H., Portinale L. (2007). Bayesian networks in reliability. Reliability Engineering and System Safety. 92(1), 92-108.

Le T.T., Chatelain F., Berenguer C. (2014). Hidden Markov Models for diagnostics and prognostics of systems under multiple deterioration modes. *European Safety and Reliability Conference - ESREL 2014*, Sep 2014, Wroclaw, Poland. Taylor & Francis - CRC Press/Balkema, pp.1197-1204

Léger A., (2009). Contribution à la formalisation unifiée des connaissances fonctionnelles et organisationnelles d'un système industriel en vue d'une évaluation quantitative des risques et de l'impact des barrières envisagées. Thèse de doctorat de Nancy Université, 28 mai, (226 pages).

Léger A., Weber P., Levrat E., Duval C., Farret R., Iung B. (2009). Methodological developments for probabilistic risk analyses of socio-technical systems. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 223(4), 313-332. DOI : 10.1243/1748006XJRR230

Léger A., Levrat E., Weber P., Iung B., Duval C., Farret R., Methodology for a probabilistic risk analysis of socio-technical systems. *Insight Journal of INCOSE,* **11**, 3, (2008), 25-26. (Article court)

Léger A., R Farret, Duval C., Levrat E., Weber P., Iung B., A safety barriers-based approach for the risk analysis of socio-technical systems. IFAC World Congress 17 (1), Coex : Korea, South, (2008a), 6938-6943.

Léger A., Duval C., R. Farret, Weber P., Levrat E., Iung B., Modeling of human and organizational impacts for system risk analyses. 9th International Probabilistic Safety Assessment and Management Conference, PSAM 9, Hong Kong, (2008b).

Léger, J.B. (1999). Contribution méthodologique à la maintenance prévisionnelle des systèmes de production : Proposition d'un cadre Formel de Modélisation. Doctorat de l'Université Henri Poincaré, Nancy I.

Limnios, N. Semi-Markov processes and reliability, Boston, Birkhauser, 2001.

Lisnianski A., Levitin G. (2003). Multi-state System Reliability: Assessment, Optimization and Applications. World Scientific, 358 pages.

Madsen A., Jensen F. (1999). LAZY propagation: A junction tree inference algorithm based on lazy inference. Articial Intelligence 113(1-2), 203-245.

Mahadevan S., Zhang R., Smith N. (2001). Bayesian networks for system reliability reassessment. Structural Safety. 23(3), 231- 251.

Manfredotti CE. (2009). Modeling and inference with relational dynamic bayesien networks. PhD, Universita di Milano – Bicocca, October, Italie.

Marquez D., Neil M., Fenton N. (2010) Improved reliability modeling using Bayesian networks and dynamic discretization. Reliability Engineering & System Safety, Volume 95, Issue 4, April 2010, Pages 412-425.

Medina-Oliva G. (2011). Modélisation d'un système de production et de son environnement technique, humain et organisationnel par Réseaux Bayésiens Orientés Objet pour le choix de stratégies de maintenance. Thèse de doctorat de Nancy Université, 12 décembre (198 pages).

Medina-Oliva G., Weber P., Iung B. (2015). Industrial system knowledge formalization to aid decision making in maintenance strategie sassessment. Engineering Applications of Artificial Intelligence, 37, 343–360.

Medina-Oliva G., Weber P., Iung B. (2013). PRM-based patterns for knowledge formalisation of industrial systems to support maintenance strategies assessment. Reliability Engineering & System Safety, August 2013, 116, 38–56.

Medina-Oliva G., Weber P., Levrat E., Iung B., Using object-oriented bayesian networks to model an industrial system: a new approach to assessing maintenance strategies. *Insight Journal of INCOSE,* 14, 4, (2011), 24-26. (Article court)

Medina-Oliva G., Weber P., Levrat E., Iung B., Use of probabilistic relational model (PRM) for dependability analysis of complex systems. 12th IFAC Symposium on Large Scale Systems: Theory and Applications, LSS 2010, Villeneuve d'Ascq : France, (2010).

Meshkat L., J.B. Dugan, F.D. Andrews (2002). Dependability analysis of systems with on-demand and active failure modes, using dynamic fault trees. IEEE Trans. On reliability, 51 (2).

Muller A., Weber P., Ben Salem A. (2004). Process model-based Dynamic Bayesian Networks for Prognostic. IEEE 4th International Conference on Intelligent Systems Design and Applications, Budapest, Hungary, August 26-28.

Munteanu P., Clerc C., Suhner M.-C., Weber P. (2007). Réseaux Bayésiens et retour d'exérience en sûreté de fonctionnement (Etat de l'art – Adaptation spécifique aux EPSdF – Elaboration de recommandations méthodologiques). Projet IMdR P04-7.

Murphy K.P., Dynamic Bayesian Networks: Representation, Inference and Learning. PhD University of California, Berkeley, (2002).

Moghaddass R., Zuo M.J., (2012). A parameter estimation method for a condition-monitored device under multi-state deterioration, Reliability Engineering & System Safety, 106, October, Pages 94-103, ISSN 0951-8320.

NF EN 61 025 (2007). - Analyse par arbre de panne (AAP).

NF EN 61 078 (2006). Techniques d'analyse pour la sûreté de fonctionnement - Bloc-diagramme de fiabilité et méthodes booléennes.

NF EN 61 165 (2006). - Application des techniques de Markov.

NF EN 62 502 (2011). Techniques d'analyse de la sûreté de fonctionnement - Analyse par arbre d'événement (AAE).

NF EN 62 551 (2013). Techniques d'analyse de sûreté de fonctionnement - Techniques des réseaux de Pétri.

Oukhellou L., Bouillaut L., Côme E., Aknin P. (2008). Combined used of sensor data and strucural information resumed by Bayesian network. Application to a railway diagnosis-aid schene, Transportation Research Part C, 16, pp 755-767.

Pascual J., Romera J., Puig V., Cembrano G., Creus R., Minoves M., (2013) Operational predictive optimal control of Barcelona water transport network, Control Engineering Practice, Volume 21, Issue 8, August 2013, Pages 1020-1034, ISSN 0967-0661, http://dx.doi.org/10.1016/j.conengprac.2013.01.009.

Pearl J. (1988). Probabilistic reasoning in intelligent systems: networks of plausible inference. Morgan Kaufmann Publishers Inc. San Francisco, USA.

Peot M., Shachter R. (1991). Fusion and propagation with multiple observations in belief networks. Articial Intelligence 48, 299-318.

Pereira E.B., Galvao R., Yoneyama T., (*2010).* Model Predictive Control using Prognosis and Health Monitoring of actuators. *IEEE International Symposium on Industrial Electronics ISIE*, pp.237,243, 4-7 July, doi: 10.1109/ISIE.2010.5637571

Portinale L., Raiteri D.C., Montani S. (2010). Supporting reliability engineers in exploiting the power of Dynamic Bayesian Networks. International Journal of Approximate Reasoning, 51(2), 179-195.

Poure P., Weber P., Theilliol D., Saadate S., (2009) Fault tolerant control of a three-phase three-wire shunt active filter system based on reliability analysis Original Research Article. Electric Power Systems Research, 79, 2, February, 325-334, DIO : 10.1016/j.epsr.2008.07.003

Rabinet L. (1989). A tutorial on hidden Markov models and selected applications in speech recognition. Proceedings of the IEEE, 77 (2), Feb.

Roblès B., Avila M., Duculty F., Vrignat P., Begot S, Kratz F. (2013). Evaluation of Minimal Data Size by Using Entropy, in a HMM Maintenance Manufacturing Use. MIM'2013 Manufacturing Modelling, Management and Control, Jun 2013, Saint Petersburg, Russia.

Russel S., Norvig P. (2010). Artificial Inteligence a modern approach (Third Edition). Prentice Hall ed., ISBN-10: 0-13-604259-7

Samé A., Bouillaut L., Aknin P., Ben Salem A. (2007). Réseaux Bayesiens Dynamiques à variable exogène continue pour la classification de point singuliers de voies ferrées, Revue d'inteligence Artificielle, 21(3), pp 353-370.

Seveso, (1982) Original Seveso directive 82/501/EEC (SEVESO I).

Shafer G. (1996). Probabilistic expert systems. Ed. SIAM (Society for Industrial and Applied Mathematics).
ISBN 978-0-89871-373-2 DOI: http://dx.doi.org/10.1137/1.9781611970043.fm

Shubin S., Zhiqiang C., Shudong S., Shenggui Z. (2010). Integrated importance measures of multi-state systems under uncertainty. Computers & Industrial Engineering 59(4), 921-928.

Simon C., Weber P., Levrat E. (2007), Bayesian Networks and Evidence Theory to Model Complex Systems Reliability, Journal of Computers, 2(1), 33-43.

Simon C., Weber P., Evsukoff A. (2008), Bayesian networks inference algorithm to implement Dempster Shafer theory in reliability analysis, Reliability Engineering and System Safety, 93(7), 950-963.

Singpurwalla. ND, Survival in Dynamic Environments. Statistical Science, Vol. 10, No. 1, 86-103, 1995.

Sommestad, T., Ekstedt, M., Johnson, P. (2010). A probabilistic relational model for security risk analysis. Computers & Security. Accepted.

SKOOB (2011) Structuring Knowledge with Object Oriented Bayesian nets (SKOOB) project. Ref. ANR PROJET 07 TLOG 021 (http://skoob.lip6.fr).

Torres-Toledano J.G., Sucar L.E., (1998) Bayesian Networks for Reliability Analysis of Complex Systems. Lecture Notes In Computer Science; Vol. 1484. Proceedings of the 6th Ibero-American Conference on AI: Progress in Artificial Intelligence. Pages: 195 – 206, ISBN:3-540-64992-1.

Verron S., Weber P., Theilliol D., T. Tiplica, A. Kobi, C. Aubrun. Decision with Bayesian network in the concurrent faults event. 7th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, Barcelona : Spain, June 30- July 3 (2009).

Verron S., Weber P., Theilliol D., T. Tiplica, A. Kobi, C. Aubrun. Using Bayesian networks for decision in the simultaneous faults case. 6th Workshop on Advanced Control and Diagnosis, Coventry : UK, November 27-28, (2008).

Villemeur A. (1988). Sûreté de fonctionnement des systèmes industriels Fiabilité – Facteurs humains Informatisation. Ed. Eyrolles, Collection de la direction des études et recherches d'électricité de France. ISSN 0399-4198

Weber P., Simon C. Réseaux bayésiens : un nouveau formalisme de modélisation pour la sûreté de fonctionnement. Dans BIVI Maîtrise des risques (2013) 1-16.

Weber P., Simon C. Réseaux bayésiens : méthodologies de modélisation en sûreté de fonctionnement. Dans BIVI Maîtrise des risques (2013) 1-29.

Weber P., Medina-Oliva G., Simon C., Iung B. (2012). Overview on Bayesian networks Applications for Dependability, Risk Analysis and Maintenance areas. Engineering Applications of Artificial Intelligence, 25, 4, June, 671-682, DOI: 10.1016/j.engappai.2010.06.002

Weber P., Becker F., Mathias A., Theilliol D., Zhang Y., (2012b). Reliability analysis of fault tolerant wind energy conversion system with doubly fed induction generator. In 5th International Conference on Intelligent Robotics and Applications, ICIRA 2012 , Montréal, Canada, octobre 2012. Published in Intelligent Robotics and Applications , Lecture Notes in Computer Science, Volume 7506, pp 483-492.

Weber P., Simon C., Theilliol D., Puig V. (2012c). Fault-tolerant control design for over-actuated system conditioned by reliability : a drinking water network application. In 8th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, SAFEPROCESS 2012 , Mexico City, Mexique, août.

Weber P., Simon C., Theilliol D., Puig V. (2011). Control allocation of k-out-of-n systems based on Bayesian Network Reliability model: Application to a drinking water network. ESREL 2011 Annual Conference, Troyes, France, September.

Weber P., Simon C., Theilliol D. (2010). Reconfiguration of over-actuated consecutive-k-out-of-n: F systems based on Bayesian Network Reliability model. 8th Workshop on Advanced Control and Diagnosis, Ferrara : Italy, November.

Weber P., Poure P., Theilliol D., Saadate S. (2008). Design of Hardware Fault Tolerant Control Architecture for Wind Energy Conversion System with DFIG based on Reliability Analysis. IEEE International Symposium on Industrial Electronics, Cambridge : UK, June 30 – July 2.

Weber P., Theilliol D., Aubrun C., 2008). Component Reliability in Fault Diagnosis Decision-Making based on Dynamic Bayesian Networks. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* 222, 2, (161-172. DOI : 10.1243/1748006XJRR96

Weber P., Theilliol D., Poure P., Saadate S., Reliability analysis in a fault tolerant control strategy dedicated to active power filter. Workshop on Advanced Control and Diagnosis, ACD'2006, Nancy, France (2006).

Weber P., Jouffe L. (2006). Complex system reliability modeling with Dynamic Object Oriented Bayesian Networks (DOOBN). Reliability Engineering and System Safety. Volume 91, Issue 2, 149-162.

Weber P., Munteanu P., Jouffe L. (2004). Dynamic Bayesian Networks modelling the dependability of systems with degradations and exogenous constraints. 11th IFAC Symposium on Information Control Problems in Manufacturing (INCOM'04). Salvador-Bahia, Brazil, April 5-7th.

Weber P., Jouffe L. (2003) Reliability modelling with Dynamic Bayesian Networks. 5th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes (SAFEPROCESS'03), Washington, D.C., USA, June 9-11.

Weber P. (2002). Dynamic Bayesian Networks model to estimate process availability. 8th International Conference Quality, Reliability, Maintenance, CCF'02. Sinaia, Romania.

Weber P., Suhner M.C., Iung B., (2001). System approach-based Bayesian Network to aid maintenance of manufacturing process. 6th IFAC Symposium on Cost Oriented Automation, Low Cost Automation, Berlin, Germany, October.

Wuillemin PH., Torti L., (2012). Structured probabilistic inference. International Journal of Approximate Reasoning, 53(7), October 2012, Pages 946-968, ISSN 0888-613X, http://dx.doi.org/10.1016/j.ijar.2012.04.004.

Welch R., Thelen T. (2000). Dynamic reliability analysis in an operational context: the Bayesian network perspective, In Dynamic reliability: future directions, Edited by: C. Smidts, J. Devooght and P.E. Labeau, ISBN 0 9652669 3 1, Maryland, USA.

Annexes

A Production de Documents pédagogiques

A.1 Synthèse quantitative

Cours	10
Sujets de Travaux Dirigés	8
Sujets de Travaux Pratiques	17

A.2 Cours (10)

Weber P. : Cours de Codage de données 1ère année (ESSTIN), depuis 2010 : « Codage de données » (174 pages), Disponible sur Arche.

Weber P. : Cours de Maintenance - Sûreté de fonctionnement 4ème année (ESSTIN), depuis 2002 : « Cours de fiabilité des systèmes industriels, outils méthodologiques pour l'analyse de la fiabilité d'un système » (110 pages), Disponible sur Arche.

Weber P. : Cours de Sûreté de fonctionnement et maîtrise des risques 5ème année (ESSTIN), depuis 2000 : « Probabilistic model in reliability / Sûreté de Fonctionnement des Systèmes Industriels » (415 pages), Cours commun au Master ISC et l'ENS Cachan depuis 2008, Disponible sur Arche.

Weber P. : Cours de Maintenance Basée sur la Fiabilité et Outils technologiques 5ème année (ESSTIN), depuis 2003 : « Maintenance Basée sur la Fiabilité » (113 pages), Disponible sur Arche.

Weber P. : Cours de Maintenance Basée sur la Fiabilité et Outils technologiques 5ème année (ESSTIN), depuis 2011 : « MBF partie 2 : outils de maintenance conditionnelle » (211 pages), Disponible sur Arche.

Weber P. : Cours de GMAO et Système d'aide au diagnostic 5ème année (ESSTIN), depuis 2003 : « SYSTEMES d'aide au Diagnostic et d'aide à la Décision » (247 pages), Disponible sur Arche.

Weber P. : Cours de Maintenance, un levier de la soutenabilité des systèmes 5ème année (ESSTIN), depuis 2012 : « Une MBF plus soutenable » (61 pages), Disponible sur Arche.

Weber P., 4h de cours : Application des Réseaux Bayésiens à l'Analyse des performances de Processus. Enseignement de cours de 3ème année à l'Ecole Centrale Paris. Présenté de 2002 à 2003.

Weber P., 4h de cours : Réseaux Bayésiens pour l'Analyse de sûreté de fonctionnement. Enseignement de cours de 3ème année à l'ENSEM filière ISA, module 582, Mise en œuvre de la sûreté de fonctionnement ; Présenté de 2004 à 2009.

Weber P., 20h de cours : "FAULT DIAGNOSIS (FDI) AND FAULT TOLERANT CONTROL (FTC) USING RELIABILITY ANALYSIS", Centro Nacional de Investigación (CENIDET) Interior Internado Palmira s/n, Col. Palmira. Cuernavaca, Morelos: Mexique, 9-14 june (2008).

A.3 Sujets de Travaux Dirigés (8)

Weber P. : Sujet de Travaux Dirigés en Codage de données 1ère année (ESSTIN), depuis 2010 : « TD 1 Codage des données et architecture des ordinateurs» (1 page), Disponible sur Arche.

Weber P. : Sujet de Travaux Dirigés en Codage de données 1ère année (ESSTIN), depuis 2010 : « TD 2 Codage des données et architecture des ordinateurs» (1 page), Disponible sur Arche.

Weber P. : Sujet de Travaux Dirigés en Codage de données 1ère année (ESSTIN), depuis 2010 : « TD 3 Codage des données et architecture des ordinateurs» (2 pages), Disponible sur Arche.

Weber P. : Sujet de Travaux Dirigés en Codage de données 1ère année (ESSTIN), depuis 2010 : « TD 4 Codage des données et architecture des ordinateurs» (3 pages), Disponible sur Arche.

Weber P. : Sujet de Travaux Dirigés en Electronique et Informatique Industrielle, 3ème années (ESSTIN), 2001 : « Méthode de Programmation structurée d'automate par réseaux à contact : commande d'une installation automatisée» (4 pages). Ce sujet n'est plus disponible sur Arche.

Weber P. : Sujet de Travaux Dirigés en Maintenance - Sûreté de fonctionnement, 4ème année (ESSTIN), 2012 : « Fiabilité des systèmes industriels : Travaux dirigés de 4A » (19 pages), Disponible sur Arche.

Weber P. : Sujet de Travaux Dirigés en Sûreté de fonctionnement des Systèmes, 5ème années (ESSTIN), 2000 : « TD Partie 1 : Arbres de Défaillances, Diagrammes de Fiabilités et Réseaux Bayésiens » (18 pages), Disponible sur Arche.

Weber P. : Sujet de Travaux Dirigés en Sûreté de fonctionnement des Systèmes, 5ème années (ESSTIN), 2000 : « TD Partie 2 : Processus de Markov » (14 pages), Disponible sur Arche.

A.4 Sujets de Travaux Pratiques (17)

Weber P. : Sujet de Travaux Pratiques de Composants technologiques 2ème année (ESSTIN), de 2001 à 2009 : « TP 1 Étude de convoyeurs» (3 pages).

Weber P. : Notice de Travaux Pratiques de Composants technologiques 2ème année (ESSTIN), de 2001 à 2009 : « TP 1 Étude de convoyeurs» (19 pages).

Weber P. : Sujet de Travaux Pratiques de Composants technologiques 2ème année (ESSTIN), de 2001 à 2009 : « TP 2 Étude du matériel pneumatique» (3 pages).

Weber P. : Notice de Travaux Pratiques de Composants technologiques 2ème année (ESSTIN), de 2001 à 2009 : « TP 2 Étude du matériel pneumatique» (7 pages).

Weber P. : Sujet de Travaux Pratiques de Composants technologiques 2ème année (ESSTIN), de 2001 à 2009 : « TP 3 Étude du matériel hydraulique» (3 pages).

Weber P. : Notice de Travaux Pratiques de Composants technologiques 2ème année (ESSTIN), de 2001 à 2009 : « TP 3 Étude du matériel hydraulique» (11 pages).

Weber P. : Sujet de Travaux Pratiques de Composants technologiques 2ème année (ESSTIN), de 2001 à 2009 : « TP 4 Étude du matériel électrique» (4 pages).
Weber P. : Notice de Travaux Pratiques de Composants technologiques 2ème année (ESSTIN), de 2001 à 2009 : « TP 4 Étude du matériel électrique» (12 pages).
Weber P. : Sujet de Travaux Pratiques de Composants technologiques 2ème année (ESSTIN), de 2001 à 2009 : « TP 5 Étude de détecteurs» (3 pages).
Weber P. : Notice de Travaux Pratiques de Composants technologiques 2ème année (ESSTIN), de 2001 à 2009 : « TP 5 Étude de détecteurs» (13 pages).
Weber P. : Sujet de Travaux Pratiques de Technologie, 2ème année (ESSTIN), de 1999 à 2001 : « Etude comparative des performances de détecteurs utilisés par des systèmes automatisés » (2 pages).
Weber P. : Sujet de Travaux Pratiques d'Automates programmables 3ème année (ESSTIN), de 2000 : « TP n° 1 : Atelier de perçage automatisé (langage à contacts et simulation Pneusim)», (2 pages).
Weber P. : Sujet de Travaux Pratiques d'Automates programmables 3ème année (ESSTIN), de 2000 : « TP n° 2 : Première approche de la programmation sur automate Siemens Série 7, partie I», (2 pages).
Weber P. : Sujet de Travaux Pratiques d'Automates programmables 3ème année (ESSTIN), de 2000 : « TP n° 3 : Première approche de la programmation sur automate Siemens Série 7, partie II», (2 pages).
Weber P. : Sujet de Travaux Pratiques d'Automates programmables 3ème année (ESSTIN), de 2000 : « TP n° 4 : Automatisation d'un poste de chargement, Grafcets maître/esclave synchronisés», (3 pages).
Weber P. : Sujet de Travaux Pratiques d'Automates programmables 3ème année (ESSTIN), de 2000 : « TP n° 5 : Automatisation d'un convoyeur à bande, modes de marche dégradé et pas à pas», (3 pages).
Weber P. : Sujet de Travaux Pratiques d'Automates programmables 3ème année (ESSTIN), de 2000 : « Notes d'accompagnement de TP Electronique et Informatique Industrielle, 3ème années ESSTIN» (18 pages).

B. Exemple de système multi-état

B.1 Présentation de l'exemple

Pour mieux cerner l'intérêt des RB appliqués à des problèmes de Sûreté de Fonctionnement, nous proposons d'analyser un système complexe multi-état. L'exemple choisi est un système complexe car il est multi-état mais il reste suffisamment simple car il est constitué de peu de composants. Cet exemple servira à montrer comment un modèle graphique probabiliste permet le calcul des grandeurs d'intérêt et comment résoudre des problèmes difficiles pour les outils de modélisation traditionnels tels que les Arbres de Défaillance, le Diagramme de Fiabilité ou encore les Chaînes de Markov.

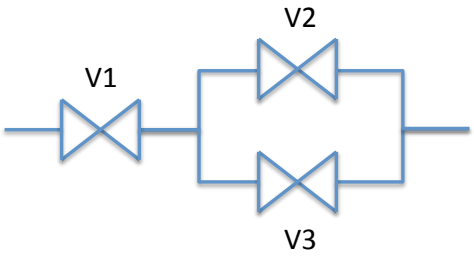


Figure 48. Système à trois vannes.

La (Figure 48) représente un système à trois vannes $(\mathrm{V1}, \mathrm{V2}, \mathrm{V3})$ utilisé pour réaliser la distribution d'un liquide. Dans ce système les composants ne sont pas définis simplement par deux états (binaires) de fonctionnement et de disfonctionnement mais par trois états : un état de fonctionnement normale $\{Ok\}$ et deux états de pannes disjointes ; i.e. un blocage en position fermé $\{Pf\}$ et un blocage en position ouvert $\{Po\}$.

En faisant l'hypothèse d'une distribution exponentielle du temps avant l'apparition d'un des états de panne des composants et en considérant les composants indépendants, nous définissons les probabilités de défaillance pour un intervalle de temps de 1 heure pour chaque état de panne des vannes :

$$\begin{array}{lll} \lambda_{1Pf} = 1 \cdot 10^{-3} & \lambda_{2Pf} = 2 \cdot 10^{-3} & \lambda_{3Pf} = 3 \cdot 10^{-3} \\ \lambda_{1Po} = 2 \cdot 10^{-3} & \lambda_{2Po} = 3 \cdot 10^{-3} & \lambda_{3Po} = 4 \cdot 10^{-3} \end{array} \quad (21)$$

La probabilité de fonctionnement d'une vanne i est donnée par une chaîne de Markov à 3 états {0, 1, 2} correspondant respectivement aux états $\{Ok, Pf, Po\}$.

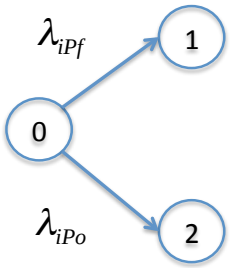


Figure 49. Chaîne de Markov d'un composant à trois états.

L'analyse combinatoire des scénarios de panne des composants fait apparaître pour le système, un ensemble de n états de fonctionnement, de fonctionnement dégradé et de panne : $n = 3^3$ *i.e.* 27 états.

Tableau 24

Scénarios	F	V1	V2	V3	ℙ (F,V1,V2,V3)
1	*Ok*	*Ok*	*Ok*	*Ok*	0,008851116
2	*Ok*	*Ok*	*Ok*	*Pf*	0,022992022
3	*Ok*	*Ok*	*Ok*	*Po*	0,030669157
4	*Ok*	*Ok*	*Pf*	*Ok*	0,01438508
5	*Ok*	*Ok*	*Pf*	*Pf*	0
6	*Ok*	*Ok*	*Pf*	*Po*	0,049844368
7	*Ok*	*Ok*	*Po*	*Ok*	0,021584119
8	*Ok*	*Ok*	*Po*	*Pf*	0,056067794
9	*Ok*	*Ok*	*Po*	*Po*	0,074789071
10	*Ok*	*Pf*	*Ok*	*Ok*	0
11	*Ok*	*Pf*	*Ok*	*Pf*	0
12	*Ok*	*Pf*	*Ok*	*Po*	0
13	*Ok*	*Pf*	*Pf*	*Ok*	0
14	*Ok*	*Pf*	*Pf*	*Pf*	0
15	*Ok*	*Pf*	*Pf*	*Po*	0
16	*Ok*	*Pf*	*Po*	*Ok*	0
17	*Ok*	*Pf*	*Po*	*Pf*	0
18	*Ok*	*Pf*	*Po*	*Po*	0
19	*Ok*	*Po*	*Ok*	*Ok*	0,012739958
20	*Ok*	*Po*	*Ok*	*Pf*	0,033093839
21	*Ok*	*Po*	*Ok*	*Po*	0
22	*Ok*	*Po*	*Pf*	*Ok*	0,020705336
23	*Ok*	*Po*	*Pf*	*Pf*	0
24	*Ok*	*Po*	*Pf*	*Po*	0
25	*Ok*	*Po*	*Po*	*Ok*	0
26	*Ok*	*Po*	*Po*	*Pf*	0
27	*Ok*	*Po*	*Po*	*Po*	0

Scénarios	F	V1	V2	V3	ℙ (F,V1,V2,V3)
28	*Hs*	*Ok*	*Ok*	*Ok*	0
29	*Hs*	*Ok*	*Ok*	*Pf*	0
30	*Hs*	*Ok*	*Ok*	*Po*	0
31	*Hs*	*Ok*	*Pf*	*Ok*	0
32	*Hs*	*Ok*	*Pf*	*Pf*	0,037367275
33	*Hs*	*Ok*	*Pf*	*Po*	0
34	*Hs*	*Ok*	*Po*	*Ok*	0
35	*Hs*	*Ok*	*Po*	*Pf*	0
36	*Hs*	*Ok*	*Po*	*Po*	0
37	*Hs*	*Pf*	*Ok*	*Ok*	0,006370119
38	*Hs*	*Pf*	*Ok*	*Pf*	0,016547283
39	*Hs*	*Pf*	*Ok*	*Po*	0,022072492
40	*Hs*	*Pf*	*Pf*	*Ok*	0,010352895
41	*Hs*	*Pf*	*Pf*	*Pf*	0,026893105
42	*Hs*	*Pf*	*Pf*	*Po*	0,035872829
43	*Hs*	*Pf*	*Po*	*Ok*	0,01553402
44	*Hs*	*Pf*	*Po*	*Pf*	0,040351808
45	*Hs*	*Pf*	*Po*	*Po*	0,05382545
46	*Hs*	*Po*	*Ok*	*Ok*	0
47	*Hs*	*Po*	*Ok*	*Pf*	0
48	*Hs*	*Po*	*Ok*	*Po*	0,044144015
49	*Hs*	*Po*	*Pf*	*Ok*	0
50	*Hs*	*Po*	*Pf*	*Pf*	0,05378503
51	*Hs*	*Po*	*Pf*	*Po*	0,071744083
52	*Hs*	*Po*	*Po*	*Ok*	0,031067358
53	*Hs*	*Po*	*Po*	*Pf*	0,080701844
54	*Hs*	*Po*	*Po*	*Po*	0,107648537

B.2 Distribution jointe

En représentant la satisfaction des objectifs du système (l'état de fonctionnement du système) par une variable aléatoire discrète F avec les états $\{Ok\}$ pour des objectifs de fonctionnements satisfaits et $\{Hs\}$ pour des objectifs de fonctionnements non satisfaits. Nous pouvons représenter la loi de probabilité jointe $\mathbb{P}(\mathrm{F}, \mathrm{V1}, \mathrm{V2}, \mathrm{V3})$ décrivant l'ensemble des combinaisons d'états des variables représentant les états de la satisfaction des objectifs

du système et les états des composants. La combinatoire des états possibles du système et celui de la satisfaction des objectifs donnent un ensemble de 54 possibilités (Tableau 24). Chacune des probabilités de la loi jointe $\mathbb{P}(\mathrm{F}, \mathrm{V1}, \mathrm{V2}, \mathrm{V3})$ correspond à la probabilité d'apparition (d'occurrence) de la situation décrite par les variables. Par exemple pour un temps $t = 500$ heures de fonctionnements le (Tableau 24) recense l'ensemble des probabilités jointes. Les paramètres du sont indépendants et la somme des valeurs de $\mathbb{P}(\mathrm{F}, \mathrm{V1}, \mathrm{V2}, \mathrm{V3})$ est égale à un.

Pour un système quelconque, nous avons un nombre de probabilités Ω correspondant au produit cartésien de toutes les variables représentants les fonctions et les composants du système (Shafer 1996, page 2). L'avantage de cette représentation est qu'elle permet de représenter de manière exhaustive l'ensemble des situations de fonctionnement et de dysfonctionnement d'un système constitué de composants multi-états. L'inconvénient majeur est sa taille qui la rend inexploitable pour un analyste dans le cas d'une application industrielle.

B.3 Calcul de la fiabilité

La fiabilité du système dépend de l'état des composants. La relation entre l'état du système et celui des composants est donnée par la fonction de structure. Ainsi, la représentation de la loi de probabilité jointe $\mathbb{P}(\mathrm{F}, \mathrm{V1}, \mathrm{V2}, \mathrm{V3})$ qui décrit l'ensemble des combinaisons d'états des variables du système permet de représenter une fonction de structure quelconque. Si nous cherchons la probabilité qu'une variable soit dans un état particulier, il suffit d'additionner toutes les probabilités des combinaisons pour lesquelles la variable est dans cet état.

Dans le cas de notre système à trois vannes, la fiabilité peut-être obtenue à partir du Tableau 24. La fiabilité du système est alors donnée par la probabilité $\mathbb{P}(\mathrm{F} = \{Ok\}) = 0{,}345721859$ c'est la somme des probabilités des scénarios de fonctionnement (1 à 27). Dans le cas présenté, seuls les scénarios (1, 2, 3, 4, 6, 7, 8, 9, 19, 20, 22) ont une probabilité différente de zéro car ce sont des états atteignables du système. Les scénarios ayant une probabilité égale à zéro sont des cas qui ne peuvent pas être réalisés compte tenu de la structure du système. A partir de la distribution de probabilité jointe il est possible de déduire toutes les probabilités conditionnelles. Malheureusement dès que le nombre de variables augmente, le tableau devient difficile à construire et à manipuler car sa taille croit de manière exponentielle.

B.4 Forme conditionnelle

A partir de cette représentation nous pouvons introduire la notion d'indépendance conditionnelle et l'exploiter pour factoriser la loi de probabilité jointe. Les composants V1, V2 et V3 sont indépendantes : $\mathbb{P}(\mathrm{V1}, \mathrm{V2}, \mathrm{V3}) = \mathbb{P}(\mathrm{V1}) \cdot \mathbb{P}(\mathrm{V2}) \cdot \mathbb{P}(\mathrm{V3})$. Cependant, l'état de fonctionnement du système $\mathbb{P}(\mathrm{F} = \{Ok\})$ dépend de l'état des composants $\mathrm{V1}, \mathrm{V2}$ et $\mathrm{V3}$. Nous pouvons alors écrire la loi de probabilité jointe sous la forme factorisée suivante :

$$\mathbb{P}(\mathrm{F}, \mathrm{V1}, \mathrm{V2}, \mathrm{V3}) = \mathbb{P}(\mathrm{V1})\ \mathbb{P}(\mathrm{V2})\ \mathbb{P}(\mathrm{V3})\ \mathbb{P}\ (\mathrm{F}|\mathrm{V1}, \mathrm{V2}, \mathrm{V3}) \quad (22)$$

Cette loi de probabilité jointe factorisée est alors définie par quatre tables :

- Les tables qui définissent la distribution de probabilité sur chacun des composants (Tableau 25, Tableau 26, Tableau 27). Ces tables représentent une distribution de probabilité sur les états de chaque composant. Cette distribution peut être définie par rapport à une durée de fonctionnement ou à une date de fin de mission. Elle est estimée à partir de la loi de fiabilité du composant (loi exponentielle, de Weibull, etc.) ou définie à partir de la simulation d'un processus aléatoire (Markovien, semi-Markovien...) ou encore donnée par un expert.
- La table qui définit la loi de probabilité conditionnelle $\mathbb{P}(\mathrm{F}, \mathrm{V1}, \mathrm{V2}, \mathrm{V3})$, Tableau 28, modélise la fonction de structure du système. Cette fonction de structure (utilisée en analyse de fiabilité) est une équation qui décrit la relation entre les états d'un système et les états des composants le constituant. Cette fonction est constante, ce qui implique une loi de probabilités conditionnelle discrète constante (indépendante du temps).

La modélisation de loi de probabilité conditionnelle définie par une TPC décrite Tableau 28 est générique et permet de modéliser des relations quelconques entre les états des composants et les états du système. De cette manière, la fonction de structure décrit l'ensemble des scénarios de fonctionnement et de dysfonctionnement du système. La TPC contient donc toute la connaissance de l'analyste.

Dans les cas plus classiques où l'hypothèse d'états binaires est faite, i.e. les composants et le système ont deux états $\{Ok, Hs\}$, la fonction de structure est une relation binaire traduite par la TPC. Il y a alors une correspondance exacte du modèle avec un diagramme de fiabilité ou un arbre de défaillance.

Dans la représentation que nous avons choisi, la fonction de structure n'est pas binaire car les composants ainsi que le système peuvent avoir plusieurs états de fonctionnements ou de dysfonctionnements. Il n'y a pas de correspondance avec une représentation par un diagramme de fiabilité ou un arbre de défaillance.

Dans l'exemple proposé comme dans tous les cas des fonctions de structures binaires, il n'y a pas d'incertitude sur la combinaison des composants conduisant au fonctionnement ou au disfonctionnement du système. Les probabilités de $\mathbb{P}(\mathrm{F}, \mathrm{V1}, \mathrm{V2}, \mathrm{V3})$ sont soit égales à zéro soit égales à un. Il s'agit d'une loi de probabilité conditionnelle déterministe. Cela n'est pas une généralité et un modèle non déterministe $\mathbb{P}(\mathrm{F}|\ \mathrm{V1}, \mathrm{V2}, \mathrm{V3}) \in [0,1]$ pourrait être formalisé. Cette représentation par une loi de probabilités conditionnelles non déterministe permet de modéliser des situations où il existe une incertitude sur la conséquence d'une

combinaison d'états de 'composants' (par exemple intégrant des opérateurs humains ou un environnement de fonctionnement variable).

Tableau 25

	$\mathbb{P}$(V1=*Ok*)	$\mathbb{P}$(V1=*Pf*)	$\mathbb{P}$(V1=*Po*)
à *t*=500	0,31655	0,22782	0,45563

Tableau 26

	$\mathbb{P}$(V2=*Ok*)	$\mathbb{P}$(V2=*Pf*)	$\mathbb{P}$(V2=*Po*)
à *t*=500	0,19748	0,32095	0,48157

Tableau 27

	$\mathbb{P}$(V3=*Ok*)	$\mathbb{P}$(V3=*Pf*)	$\mathbb{P}$(V3=*Po*)
à *t*=500	0,14159	0,3678	0,49061

Tableau 28

V1	V2	V3	$\mathbb{P}$(F=*Ok*)	$\mathbb{P}$(F=*Hs*)
Ok	*Ok*	*Ok*	1	0
Ok	*Ok*	*Pf*	1	0
Ok	*Ok*	*Po*	1	0
Ok	*Pf*	*Ok*	1	0
Ok	*Pf*	*Pf*	0	1
Ok	*Pf*	*Po*	1	0
Ok	*Po*	*Ok*	1	0
Ok	*Po*	*Pf*	1	0
Ok	*Po*	*Po*	1	0
Pf	*Ok*	*Ok*	0	1
Pf	*Ok*	*Pf*	0	1
Pf	*Ok*	*Po*	0	1
Pf	*Pf*	*Ok*	0	1
Pf	*Pf*	*Pf*	0	1
Pf	*Pf*	*Po*	0	1
Pf	*Po*	*Ok*	0	1
Pf	*Po*	*Pf*	0	1
Pf	*Po*	*Po*	0	1
Po	*Ok*	*Ok*	1	0
Po	*Ok*	*Pf*	1	0
Po	*Ok*	*Po*	0	1
Po	*Pf*	*Ok*	1	0
Po	*Pf*	*Pf*	0	1
Po	*Pf*	*Po*	0	1
Po	*Po*	*Ok*	0	1
Po	*Po*	*Pf*	0	1
Po	*Po*	*Po*	0	1

B.5 Factorisation

L'équation (1) est une factorisation de la loi de probabilité jointe $\mathbb{P}(\mathrm{F}, \mathrm{V1}, \mathrm{V2}, \mathrm{V3})$. La loi de probabilités conditionnelle déterministe $\mathbb{P}(\mathrm{F}|\mathrm{V1}, \mathrm{V2}, \mathrm{V3})$ reste de dimension importante. Il est intéressant de remarquer que nous pouvons simplifier cette loi en introduisant des variables intermédiaires supplémentaires comme nous le faisons lors de la construction d'un arbre de défaillance. Par exemple, en séparant le système en deux étages comme illustré à la Figure 50.

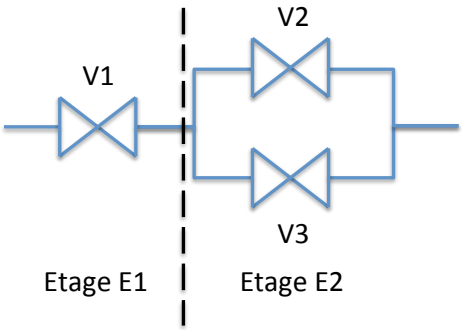


Figure 50. Décomposition du système à trois vannes.

Nous ajoutons les variables E1 et E2 qui permettent de caractériser les étages E1 et E2 du système. La variable E1 caractérise la possibilité de commander le passage du fluide sur l'étage 1, de même pour E2 sur l'étage 2.

Tableau 29

V1	$\mathbb{P}$(E1=*Ok*)	$\mathbb{P}$(E1=*Pf*)	$\mathbb{P}$(E1=*Po*)
Ok	1	0	0
Pf	0	1	0
Po	0	0	1

Tableau 30

V2	V3	$\mathbb{P}$(E2=Ok)	$\mathbb{P}$(E2=Pf)	$\mathbb{P}$(E2=Po)
Ok	*Ok*	1	0	0
	Pf	1	0	0
	Po	0	0	1
Pf	*Ok*	1	0	0
	Pf	0	1	0
	Po	0	0	1
Po	*Ok*	0	0	1
	Pf	0	0	1
	Po	0	0	1

Tableau 31

E1	E2	$\mathbb{P}$(F=*Ok*)	$\mathbb{P}$(F=*Hs*)
Ok	*Ok*	1	0
	Pf	0	1
	Po	1	0
Pf	*Ok*	0	1
	Pf	0	1
	Po	0	1
Po	*Ok*	1	0
	Pf	0	1
	Po	0	1

Pour conserver toute l'information nécessaire, nous définissons E1 et E2 sur trois états :

- $\{Ok\}$ s'il est possible de commander l'ouverture et la fermeture de l'étage,
- $\{Pf\}$ si l'étage est défaillant et ferme le circuit ne laissant ainsi plus passer de fluide,

- $\{Po\}$ si l'étage est défaillant et reste toujours ouvert laissant passer le fluide en permanence.

L'équation (1) s'écrit alors sous une nouvelle forme factorisée :

$$\mathbb{P}(\mathrm{F}, \mathrm{V1}, \mathrm{V2}, \mathrm{V3}) = \mathbb{P}(\mathrm{V1})\mathbb{P}(\mathrm{V2})\mathbb{P}(\mathrm{V3})\ \mathbb{P}(\mathrm{E1}|\mathrm{V1})\ \mathbb{P}(\mathrm{E2}|\mathrm{V2}, \mathrm{V3})\ \mathbb{P}(\mathrm{F}|\mathrm{E1}, \mathrm{E2}) \qquad (23)$$

Les distributions de probabilités sur les états des composants restent inchangées par rapport au cas précédent (Tableau 25, Tableau 26, Tableau 27), seule la distribution conditionnelle est décomposée en plusieurs distributions. Les nouvelles lois de probabilités conditionnelles sont définies par les (Tableau 18, Tableau 19, Tableau 20).

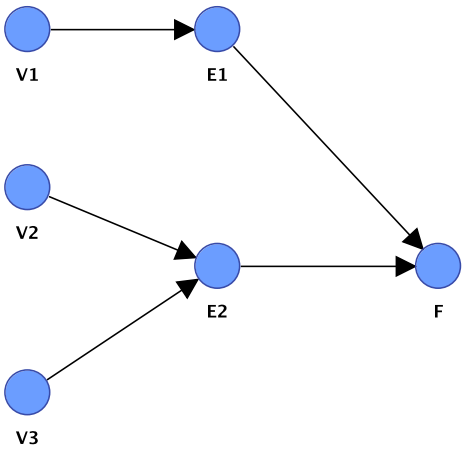


Figure 51. Présentation graphique de la loi jointe factorisée : modélisation par RB

Le principe de factorisation permet de simplifier le modèle par un ensemble de lois de probabilités conditionnelles dont la taille est largement inférieure à celle de la loi de probabilité jointe. Un réseau Bayésien est donc une représentation graphique de cette loi de probabilité jointe factorisée, ajoutant à la représentation compacte, la formalisation graphique qui facilite son interprétation (Figure 51). Nous retrouvons ici un avantage majeur des RB. Il faut noter qu'il n'y a pas de raison de passer par la loi jointe et qu'une construction graduelle du RB permet de formaliser directement la représentation factorisée.

B.6 Inference

Enfin, les algorithmes d'inférence exacte calculent la loi de probabilité marginale de chaque variable tout comme la loi de probabilité de F :

$$\begin{aligned} \mathbb{P}(\mathrm{F} = Ok) &= 0{,}345721859 \\ \mathbb{P}(\mathrm{F} = Hs) &= 0{,}654278141 \end{aligned} \qquad (24)$$

Nous retrouvons la somme des scénarios 1 à 27 de la loi jointe présentée Tableau 24 pour le calcul de $\mathbb{P}(\mathrm{F} = Ok)$.

C. Modélisation par RB dans le cas booléen

La représentation de l'échec de la mission d'un système d'une façon probabiliste représente naturellement l'incertitude aléatoire. Pour une telle représentation, nous considérons le comportement de processus comme une variable aléatoire qui prend ses valeurs dans un espace fini d'états correspondant à ceux du système et de ses composants.

C.1 Présentation des notations

Pour un système constitué de r composants (ou éléments), l'état du système dépend de la configuration des composants selon la fonction de structure. Considérons que les états de fonctionnement et de dysfonctionnement des composants sont représentés par une variable $x_i, i = \{1, \dots r\}$. Cette variable peut classiquement prendre les valeurs suivantes (Villemeur 1988 p. 158 ; Cocozza-Thivent 1997 p. 231):

$$\begin{aligned} x_i &= 0 \text{ le composant } i \text{ est en fonctionnement} \\ x_i &= 1 \text{ le composant } i \text{ est en panne} \end{aligned} \tag{25}$$

Le système est modélisé par une variable y qui prend les valeurs suivantes :

$$\begin{aligned} y &= 0 \text{ le système est en fonctionnement} \\ y &= 1 \text{ le système est en panne} \end{aligned} \tag{26}$$

Remarque : les auteurs (Corazza 1975 p. 114 ; Gertsbakh 2000 p. 1) utilisent une convention inverse.

Nous utilisons cette convention qui permet l'extension aux cas multi-état. Le système est modélisé par une variable booléenne. La fonction de structure ϕ est une fonction binaire liant les états des composants aux états du système telle que :

$$y = \phi(x) \tag{27}$$

où $x = (x_1, x_2, \dots, x_r)$. La fonction ϕ prend les états 0 si le système fonctionne et 1 si le système est en panne. Cette fonction de structure peut être définie aisément à partir des coupes minimales ou des liens (chemins de succès) minimaux.

Les coupes minimales, notées C_j, sont les scénarios de dysfonctionnement. Elles sont définies à partir des plus petits ensembles de composants en panne qui ne permettent pas

au système de fonctionner. Les liens minimaux, noté L_j, sont les scénarios de fonctionnement du système définis à partir des plus petits ensembles de composants en fonction qui permettent le fonctionnement du système (Villemeur 1988).

A partir des coupes minimales, la fonction de structure s'écrit :

$$\phi(x) = 1 - \prod_{C_j} \left[1 - \prod_{x_i \in C_j} (x_i) \right] \tag{28}$$

A partir des liens minimaux, la fonction de structure s'écrit :

$$\phi(x) = \prod_{L_j} \left[1 - \prod_{x_i \in L_j} (1 - x_i) \right] \tag{29}$$

La fiabilité du système est donc la probabilité que celui-ci soit fonctionnel *i.e.* $\mathbb{P}(y = 0)$ ou encore $\mathbb{P}(\phi(x) = 0)$.

C.2 Construction du modèle Réseau Bayésien par les liens ou les coupes minimales

Une représentation de la fonction de structure est facilement transposable en RB. Nous proposons de l'illustrer sur le système de distribution de fluide dont le diagramme de fiabilité est donné Figure 52.

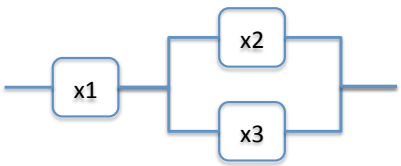


Figure 52 : Diagramme de fiabilité du système de distribution de fluide

En considérant que les composants n'ont que 2 états : $x_i = 0$ si la vanne i fonctionne et laisse passer le fluide et $x_i = 1$ si la vanne i ne laisse pas passer le fluide. Les distributions de probabilités des x_i sont données (Tableau 32).

Tableau 32

	$\mathbb{P}(x_i = 0)$	$\mathbb{P}(x_i = 1)$
x_1	0,77218	0,22782
x_2	0,67905	0,32095
x_3	0,6322	0,3678

Il existe alors deux liens minimaux :

$$L_1 = \{x_1, x_2\}$$
$$L_2 = \{x_1, x_3\} \quad (30)$$

Pour calculer la probabilité de bon fonctionnement, nous pouvons appliquer le théorème de Sylvester-Poincaré :

$$\mathbb{P}(y = 0) = \mathbb{P}(L_1) + \mathbb{P}(L_2) - \mathbb{P}(L_1 \cap L_2) \quad (31)$$

avec :
$\mathbb{P}(L_1) = \mathbb{P}(x_1 = 0) \cdot \mathbb{P}(x_2 = 0)$
$\mathbb{P}(L_2) = \mathbb{P}(x_1 = 0) \cdot \mathbb{P}(x_3 = 0)$
$\mathbb{P}(L_1 \cap L_2) = \mathbb{P}(x_1 = 0) \cdot \mathbb{P}(x_2 = 0) \cdot \mathbb{P}(x_3 = 0)$

L'application numérique donne :

$$\mathbb{P}(y = 0) = 0{,}681027695 \quad (32)$$

Remarque : Nous ne retrouvons pas le résultat éq. (24) car nous n'avons pas modélisé le blocage en position ouverte du système.

Tableau 33

x_1	x_2	$\mathbb{P}(L_1$=0)	$\mathbb{P}(L_1$=1)
0	0	1	0
	1	0	1
1	0	0	1
	1	0	1

Tableau 34

x_1	x_3	$\mathbb{P}(L_2$=0)	$\mathbb{P}(L_2$=1)
0	0	1	0
	1	0	1
1	0	0	1
	1	0	1

Tableau 35

L_1	L_2	$\mathbb{P}(y$=0)	$\mathbb{P}(y$=1)
0	0	1	0
	1	1	0
1	0	1	0
	1	0	1

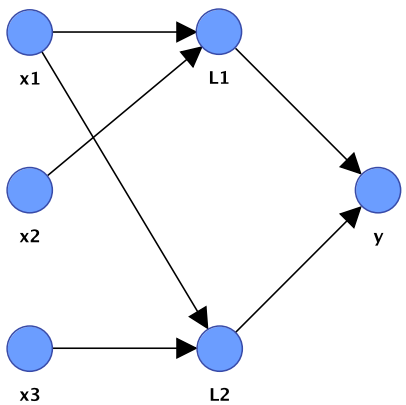


Figure 53 : RB modélisant les relations de dépendances entre les liens minimaux du système.

Pour définir un RB équivalent, nous définissons une variable pour chaque lien minimal, les parents des liens sont les variables dont ils dépendent : pa $(L_1) = \{x_1, x_2\}$ et pa $(L_2) = \{x_1, x_3\}$. Le lien existe ou fonctionne $(L_j = 0)$ si les composants le constituant sont dans un

état de fonctionnement $(x_i = 0)$. Nous pouvons traduire cela par la TPC (Tableau 33 et Tableau 34). Le système est défini en fonction des états des liens minimaux. S'il existe l'occurrence d'au moins un lien minimal alors le système est dans un état de fonctionnement. Ceci est définit par la TPC (Tableau 35). La structure du RB est donnée par la Figure 53, il encode exactement l'équation (29).

Par inférence, le RB calcule, à partir des distributions associées aux composants x_i (Tableau 32), la distribution marginale sur la variable y, et les liens minimaux L_i (Tableau 36). Nous obtenons pour $\mathbb{P}(y = 0)$ la même valeur que pour l'équation (24).

Tableau 36

y	
0	0,681027695
1	0,318972305

L_1	
0	0,524348829
1	0,475651171

L_2	
0	0,488172196
1	0,511827804

Le même raisonnement est fait à partir des coupes minimales. Il existe, pour le système, deux coupes minimales:

$$\begin{aligned} C_1 &= \{x_1\} \\ C_2 &= \{x_2, x_3\} \end{aligned} \tag{33}$$

Pour calculer la probabilité de mauvais fonctionnement, nous pouvons de nouveau appliquer le théorème de Sylvester-Poincaré :

$$\mathbb{P}(y = 1) = \mathbb{P}(C_1) + \mathbb{P}(C_2) - \mathbb{P}(C_1 \cap C_2) \tag{34}$$

avec :
$\mathbb{P}(C_1) = \mathbb{P}(x_1 = 1)$
$\mathbb{P}(C_2) = \mathbb{P}(x_2 = 1) \cdot \mathbb{P}(x_3 = 1)$
$\mathbb{P}(C_1 \cap C_2) = \mathbb{P}(x_1 = 1) \cdot \mathbb{P}(x_2 = 1) \cdot \mathbb{P}(x_3 = 1)$

L'application numérique donne :

$$\mathbb{P}(y = 1) = 0{,}318972305 \tag{35}$$

Pour définir un RB équivalent, il suffit de définir une variable pour chaque coupe minimale. Les parents des coupes sont les variables dont ils dépendent. Une coupe empêche le système de fonctionner $(C_j = 1)$ si les composants la constituant sont dans un état de dysfonctionnement $(x_i = 1)$. Les TPC sont définies (Tableau 37, Tableau 38). L'état du système est défini en fonction des états des coupes minimales. S'il existe l'occurrence d'au moins une coupe minimale alors le système est dans un état de dysfonctionnement

$\mathbb{P}(y = 1)$ (Tableau 39). La structure du modèle par RB est présentée (Figure 54), il encode l'équation (28).

Tableau 37

x_1	$\mathbb{P}(C_1$=0)	$\mathbb{P}(C_1$=1)
0	1	0
1	0	1

Tableau 38

x_2	x_3	$\mathbb{P}(C_2$=0)	$\mathbb{P}(C_2$=1)
0	0	1	0
	1	1	0
1	0	1	0
	1	0	1

Tableau 39

C_1	C_2	$\mathbb{P}(y$=0)	$\mathbb{P}(y$=1)
0	0	1	0
	1	0	1
1	0	0	1
	1	0	1

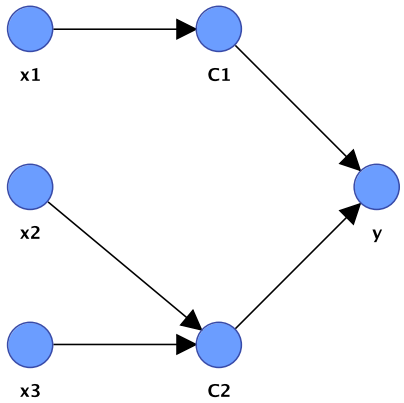


Figure 54 : RB modélisant les relations de dépendances entre les coupes minimales et le système.

Par inférence, le RB calcule, à partir des distributions associées aux composants x_i (Tableau 32), la distribution marginale sur la variable y, et les coupes minimales C_i (Tableau 40). Nous obtenons pour $\mathbb{P}(y = 1)$ la même valeur que pour l'éq. (24).

Tableau 40

y	
0	0,681027695
1	0,318972305

C_1	
0	0,77218
1	0,22782

C_2	
0	0,88195459
1	0,11804541

Les deux méthodes de modélisation utilisées ici donnent des résultats identiques. Le lecteur pourra calculer la loi jointe pour confirmer que les deux modèles sont équivalents. Il faut également noter que les TPC ont des formes standard OU et ET que l'on peut reconnaitre dans le RB encodant les liens minimaux ou les coupes minimales. Enfin, il est à noter que si l'analyste encode des liens (resp. coupes) plutôt que liens minimaux (resp. coupes minimales) le résultat n'est pas affecté, la structure du modèle est simplement plus lourde.

C.3 Construction du Réseau Bayésien par une approche descendante

Dans le cas de grands systèmes l'énumération de tous les scénarios de fonctionnement ou de dysfonctionnement est fastidieuse. Pour résoudre ce problème la technique de construction de modèles par Arbre de Défaillance est fondée sur le principe d'analyse descendante d'un évènement sommet vers les évènements élémentaires (racines ou

feuilles). La structure du RB peut être déduite à partir d'une démarche identique, ou directement à partir d'un arbre de défaillance existant.

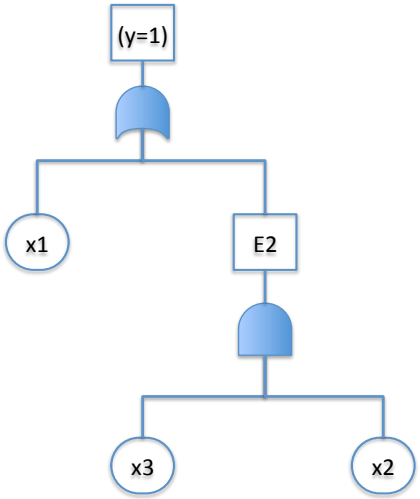


Figure 55 : Arbre de défaillance du système de distribution de fluide.

Pour construire un RB équivalent à l'arbre de défaillance présenté Figure 55, une variable aléatoire discrète est définie pour chaque événement. Les parents des évènements sont les variables dont ils dépendent. La TPC permettant de définir l'évènement (E_j) est construite en fonction des portes logiques (ET, OU, k/n, etc.) apparaissant dans l'arbre de défaillance.

Remarque : *Toutes les portes logiques peuvent être représentées dans un RB (portes k/n, OU exclusif, …). Pour cela, il suffit simplement de retranscrire la table de vérité de la fonction logique dans la TPC (Simon et al. 2007 ; Simon et al. 2008). La prise en compte de contraintes topologiques comme dans les systèmes k/n consécutifs linéaires ou circulaires non modélisable par arbres de défaillances est également réalisable (Weber et al. 2010 ; Weber et al. 2011).*

Tableau 41

x_2	x_3	$\mathbb{P}(E_2 = 0)$	$\mathbb{P}(E_2 = 1)$
0	0	1	0
	1	1	0
1	0	1	0
	1	0	1

Tableau 42

x_1	E_2	$\mathbb{P}(y = 0)$	$\mathbb{P}(y = 1)$
0	0	1	0
	1	0	1
1	0	0	1
	1	0	1

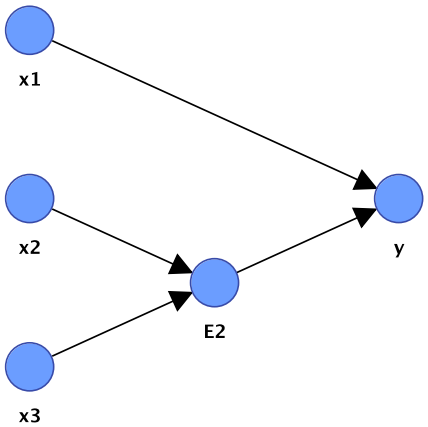


Figure 56 : RB modélisant les relations de dépendances des évènements de l'arbre de défaillance.

Par exemple, pour une porte ET, $(\boldsymbol{E_2 = x_2 \wedge x_3})$ si les deux composants sont défaillants $(\boldsymbol{x_i = 1})$ alors l'événement $\boldsymbol{E_2}$ est occurrent c'est à dire $\boldsymbol{E_2 = 1}$ (Tableau 41). Une porte OU est modélisée (Tableau 42).

Par calcul dans l'arbre de défaillance :

$$\mathbb{P}(y = 1) = 0{,}318972305 \quad (36)$$
$$\mathbb{P}(E_2 = 1) = 0{,}11804541 \quad (37)$$

L'événement redouté du système $(\boldsymbol{y = 1})$ est défini en fonction des états de $\boldsymbol{E_2}$ et du composent $\boldsymbol{x_1}$: $(\boldsymbol{y = x_1 \vee E_2})$. Si $(\boldsymbol{x_1 = 1})$ ou $(\boldsymbol{E_2 = 1})$ alors le système est dans un état de dysfonctionnement $(\boldsymbol{y = 1})$. La TPC correspondante est donnée (Tableau 41). Le RB a la structure présentée par la Tableau 42.

Par inférence, le RB calcule à partir des distributions associées aux composants x_i (Tableau 32), la distribution sur la variable y, et la probabilité d'occurrence de l'événement E_2 (24). Nous obtenons la même valeur que pour éq. (24) et (Tableau 43).

Tableau 43

y	
0	0,681027695
1	0,318972305

E_2	
0	0,88195459
1	0,11804541

D. Modélisation par RB dans le cas multi-état

Dans le cas de systèmes Multi-états les techniques de modélisation en sûreté de fonctionnement proposées dans la littérature sont assez difficiles à mettre en œuvre (Lisnianski et Levitin 2003). Nous allons montrer dans cette partie que, en appliquant la même démarche de construction de modèle que nous l'avons fait en binaire nous pouvons formaliser des modèles multi-états sous la forme de réseaux bayésien, les explications détaillées sont données dans l'annexe C. Nous montrerons en suite qu'il est possible d'utiliser une démarche de construction sur le principe d'analyse descendante d'un évènement sommet vers les évènements élémentaires tels que celle formalisée pour la construction des arbres de défaillances. Cette technique de modélisation est le résultat de l'analyse et de la prise de recule sur les méthode que nous avons initié dans l'article Weber et al. (2001), Muller et al (2004), Weber et Jouffe (2006), puis dans les travaux de doctorat de Gabriela Medina Oliva (2011) et au cours du projet ANR SKOOB.

D.1 Formalisation des variables

Dans le cas d'un système multi-état, il est nécessaire de modéliser plus de deux états pour définir les états de fonctionnement des composants. Nous définissons alors les variables qui représentent les composants (Shubin et al. 2010) :

$x_i = 0$ si le composant i est en fonctionnement normal (bon fonctionnement),
$x_i = \{1 \dots (l_i - 1)\}$ si le composant i est dans un état de fonctionnement dégradé, (38)
$x_i = \{l_i \dots n_i\}$ si le composant i est dans un état de dysfonctionnement,

avec l_i le premier état de panne du composant, c'est à dire que le composant ne satisfait plus les objectifs de fonctionnement attendu dans le système.

Les états $\{1 \dots (l_i - 1)\}$ sont des états de fonctionnement dégradés c'est à dire que le composant n'est pas en état de bon fonctionnement, il est altéré ou dégradé, mais il n'empêche pas l'atteinte des objectifs de fonctionnement du système. Les états $\{l_i \dots n_i\}$ sont des états de panne du composant qui peuvent avoir des conséquences différentes sur le système. Ces états peuvent être mis en relation avec les modes de défaillances observés sur le système.

***Remarque** : les auteurs (Lisnianski and Levitin 2003 chapitre 2), utilisent une convention différente en relation avec la notion de capacité des composants (resp. du système) 0 pour*

une capacité nulle de réaliser la mission et une valeur croissante pour une capacité croissante de réaliser des objectifs.

Le système est lui aussi défini par une variable multi-état en relation avec les scénarios de fonctionnement et les scénarios de dysfonctionnement du système. Le système est modélisé par une variable y qui prend les valeurs suivantes :

$y = 0$ correspond au fonctionnement normal (bon fonctionnement),
$y = \{1 \dots (l-1)\}$ correspond à un état de fonctionnement dégradé, (39)
$y = \{l \dots n\}$ correspond à des états de dysfonctionnement du système.

Il est alors difficile de représenter un tel système par un arbre de défaillance ou un digramme de fiabilité. Cependant, les notions de coupes minimales et de chemins de succès permettent de définir totalement les relations entre les états du système et les états des composants. Il s'agit donc de l'élaboration d'une fonction de structure ϕ multi-état (non binaire) et considère les états 0 à n du système. La fonction ϕ permet de relier les états des composants aux états du système telle que $y = \phi(x)$, où $x = (x_1, x_2, \dots, x_r)$.

D.2 Construction du modèle Réseau Bayésien

Un RB est une représentation compacte et probabilisée de la fonction de structure multi-état du système. Les variables du RB modélisent les états des composants et du système. Il reste à structurer le modèle pour encoder les scénarios de fonctionnement et de dysfonctionnement.

Une première solution consiste à faire la liste des liens minimaux ou des coupes minimales. En appliquant la même démarche que dans le cas booléen, nous définissons un RB qui représente les dépendances conditionnelles reliant le fonctionnement ou le dysfonctionnement du système aux coupes ou aux liens minimaux. Le principe de construction est illustré sur le système de la Figure 8. Pour ce système, il existe 7 scénarios pour lesquels le système est dans un état de fonctionnement ($y = 0$). Pour rappel, les trois états que peut prendre chaque composant :

0 correspond à $\{Ok\}$, 1 correspond à $\{Pf\}$, 2 correspond à $\{Po\}$. (40)

Les liens minimaux permettant le fonctionnement du système sont définis à partir des combinaisons d'état des composants suivantes :

$$\begin{aligned} L_1 &= \{x_1 = 0, x_2 = 0\} \\ L_2 &= \{x_1 = 0, x_3 = 0\} \\ L_3 &= \{x_1 = 0, x_2 = 2\} \\ L_4 &= \{x_1 = 0, x_3 = 2\} \\ L_5 &= \{x_1 = 2, x_2 = 0, x_3 = 0\} \\ L_6 &= \{x_1 = 2, x_2 = 1, x_3 = 0\} \end{aligned} \quad (41)$$

$$L_7 = \{x_1 = 2, x_2 = 0, x_3 = 1\}$$

Il est possible de construire un RB à partir des ces 7 scénarios en définissant une variable pour chaque scénario de fonctionnement ($L_1 \dots L_7$). Le lien existe ou fonctionne $(L_j = 0)$ si les composants le constituant sont dans l'état spécifié dans le lien L_j. S'il existe au moins un lien minimal tel que $\left(L_j = 0\right)$ alors le système fonctionne $(y = 0)$. En reliant y à chaque lien minimal et en liant chaque lien minimal L_j aux variables x_i apparaissant dans le lien nous obtenons la structure du RB de la Figure 57.

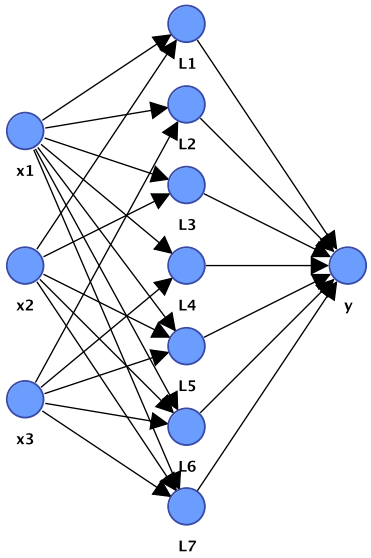


Figure 57 : RB structuré par les liens minimaux pour un système multi-état.

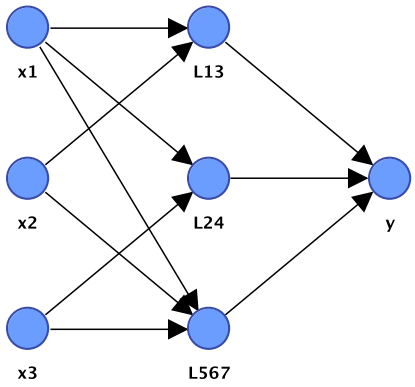


Figure 58 : RB compact, structuré par les liens minimaux pour un système multi-état.

Cette approche permet de générer le RB automatiquement mais conduit rapidement à un modèle peu compact et donc peu lisible. Il est alors judicieux de factoriser le réseau en fusionnant les nœuds représentant des liens minimaux connectés aux mêmes variables tels que $\{L_1, L_3\}$, $\{L_2, L_4\}$ et $\{L_5, L_6, L_7\}$ en créant des variables représentant des liens minimaux complexes et en utilisant pleinement les capacités des TPC basées sur une logique de combinaisons multi-états. Pour le cas $\{L_1, L_3\}$ nous définissons : $L_{13} = \{L_1 \cup L_3\}$, $L_{13} = 0$ pour les deux scénarios : $L_1 = \{x_1 = 0, x_2 = 0\}$ et $L_3 = \{x_1 = 0, x_2 = 2\}$; dans tous les autres cas $L_{13} = 1$ (Tableau 44). Pour L_{24} la TPC est définie de la même manière et est identique (Tableau 45). Enfin pour L_{567} la variable est dans l'état 0 pour les trois scénarios : $L_5 = \{x_1 = 2, x_2 = 0, x_3 = 0\}$, $L_6 = \{x_1 = 2, x_2 = 1, x_3 = 0\}$, $L_7 = \{x_1 = 2, x_2 = 0, x_3 = 1\}$ tel qu'il est défini dans le (Tableau 46). La structure plus compacte du RB est présentée à la (Figure 20).

En relation avec (Tableau 25, Tableau 26, Tableau 27), les distributions de probabilités sur les variables x_i sont définies dans le (Tableau 47). Par inférence dans le RB, nous retrouvons

pour y les valeurs de la loi de probabilité donnée à l'éq. (24) ainsi que les probabilités de fonctionnements des liens L_i (Tableau 48).

Tableau 44

x_1	x_2	$\mathbb{P}(L_{13}=0)$	$\mathbb{P}(L_{13}=1)$
0	0	**1**	**0**
	1	0	1
	2	**1**	**0**
1	0	0	1
	1	0	1
	2	0	1
2	0	0	1
	1	0	1
	2	0	1

Tableau 45

x_1	x_3	$\mathbb{P}(L_{24}=0)$	$\mathbb{P}(L_{24}=1)$
0	0	**1**	**0**
	1	0	1
	2	**1**	**0**
1	0	0	1
	1	0	1
	2	0	1
2	0	0	1
	1	0	1
	2	0	1

Tableau 46

x_1	x_2	x_3	$\mathbb{P}(L_{567}=0)$	$\mathbb{P}(L_{567}=1)$
0	0	0	0	1
		1	0	1
		2	0	1
	1	0	0	1
		1	0	1
		2	0	1
	2	0	0	1
		1	0	1
		2	0	1
1	0	0	0	1
		1	0	1
		2	0	1
	1	0	0	1
		1	0	1
		2	0	1
	2	0	0	1
		1	0	1
		2	0	1
2	0	0	**1**	**0**
		1	**1**	**0**
		2	0	1
	1	0	**1**	**0**
		1	0	1
		2	0	1
	2	0	0	1
		1	0	1
		2	0	1

Tableau 47

x_1	
0	0,31655
1	0,22782
2	0,45563

x_2	
0	0,19748
1	0,32095
2	0,48157

x_3	
0	0,14159
1	0,3678
2	0,49061

Tableau 48

y	
0	0,345721859
1	0,654278141

L_{13}	
0	0,214953278
1	0,785046723

L_{24}	
0	0,20012291
1	0,79987709

L_{567}	
0	0,066539133
1	0,933460867

Tableau 49

x_1	$\mathbb{P}(C_1 = 0)$	$\mathbb{P}(C_1 = 1)$
0	1	0
1	**0**	**1**
2	1	0

Tableau 50

x_2	x_3	$\mathbb{P}(C_2 = 0)$	$\mathbb{P}(C_2 = 1)$
0	0	1	0
	1	1	0
	2	1	0
1	0	1	0
	1	**0**	**1**
	2	1	0
2	0	1	0
	1	1	0
	2	1	0

Tableau 51

x_1	x_2	$\mathbb{P}(C_3 = 0)$	$\mathbb{P}(C_3 = 1)$
0	0	1	0
	1	1	0
	2	1	0
1	0	1	0
	1	1	0
	2	1	0
2	0	1	0
	1	1	0
	2	**0**	**1**

Tableau 52

x_1	x_3	$\mathbb{P}(C_4 = 0)$	$\mathbb{P}(C_4 = 1)$
0	0	1	0
	1	1	0
	2	1	0
1	0	1	0
	1	1	0
	2	1	0
2	0	1	0
	1	1	0
	2	**0**	**1**

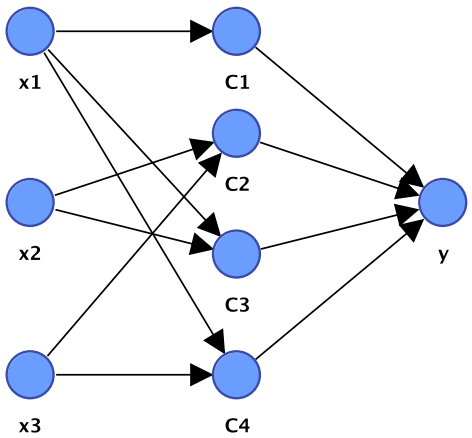


Figure 59 : RB structuré par les coupes minimales pour un système multi-état.

D.3 Construction du modèle Réseau Bayésien par les coupes minimales

La même démarche est appliquée à partir des coupes minimales. Les quatre scénarios de dysfonctionnement sont les suivants :

$$\begin{aligned} C_1 &= \{x_1 = 1\} \\ C_2 &= \{x_2 = 1, x_3 = 1\} \\ C_3 &= \{x_1 = 2, x_2 = 2\} \\ C_4 &= \{x_1 = 2, x_3 = 2\} \end{aligned} \tag{42}$$

C_1, la vanne V1 est dans l'état $\{Pf\}$ aucun fluide ne peut circuler,
C_2, les vannes V2 et V3 sont dans l'état $\{Pf\}$ aucun fluide ne peut circuler,
C_3, les vannes V1 et V2 sont dans l'état $\{Po\}$ le fluide ne peut pas être arrêté,
C_4, les vannes V1 et V3 sont dans l'état $\{Po\}$ le fluide ne peut pas être arrêté.

Dans ce cas nous ne pouvons pas fusionner les variables modélisant les coupes car elles sont connectées à des variables différentes. Les TPC sont données dans les (Tableau 49, Tableau 50, Tableau 51, Tableau 52). La structure du modèle est présentée (Figure 59). Cette structure est très compacte et exploite la puissance de modélisation des RB.

Par inférence dans le RB avec les distributions de probabilité sur les variables x_i définies (Tableau 53), nous calculons les distributions de y ainsi que des coupes C_1 à C_4 (Tableau 17). Nous retrouvons pour y les valeurs de la loi de probabilité éq. (3).

Tableau 53

y	
0	0,345721859
1	0,654278141

C_1	
0	0,77218
1	0,22782

C_2	
0	0,88195459
1	0,11804541

C_3	
0	0,780582261
1	0,219417739

C_4	
0	0,776463366
1	0,223536634

Comme nous l'avons vu, à partir des liens ou des coupes minimales, il est toujours possible de construire un RB que cela soit pour des systèmes simples, complexes, binaires ou multi-états. Les modèles des figures (Figure 57 , Figure 59, Figure 59) sont strictement équivalents car ils modélisent la même distribution jointe. Une construction automatique est envisageable. Cependant, les modèles ainsi obtenus sont de grande dimension et n'ont pas une structure très explicite. Cette structuration en trois couche : composants ; coupes ou liens minimaux ; missions du système, n'est pas très lisible dans le cas de systèmes de grandes dimensions tels les systèmes industriels.

D.4 Construction depuis une analyse fonctionnelle/dysfonctionnelle

Nous pouvons construire des modèles graphiques probabilistes multi-états sans passer par cette étape fastidieuse de description de tous les scénarios de fonctionnement ou de dysfonctionnement tels que les méthodes construites sur le principe d'analyse des coupes minimales et des liens minimaux.

Pour obtenir un modèle plus lisible, la démarche de construction des Arbres de défaillances est intéressante car elle fait apparaître des événements intermédiaires rattachés à une sémantique traduisant des situations de fonctionnement et de dysfonctionnement du système. Malheureusement, cette démarche est peu adaptée à des modèles multi-états.

Il est donc intéressant d'aborder la construction du modèle sur la base d'une analyse fonctionnelle couplée avec une analyse dysfonctionnelle comme nous l'avons proposé dans les articles (Weber et al. 2001 ; Muller et al. 2004 ; Weber et Jouffe 2006 ; Medina-Oliva et al., 2013). Cette démarche permet de structurer des modèles RB pour des systèmes multi-états. L'analyse fonctionnelle permet de spécifier les variables structurant le modèle selon des niveaux d'abstraction décrits par une architecture fonctionnelle. Les analyses AMDEC et HAZOP permettent de spécifier les états des variables représentant les composants (états de marche, états de marche dégradée, états de panne) et les fonctions du système (modes de fonctionnement, modes de défaillance).

L'analyse fonctionnelle permet de décomposer le système en faisant apparaître les fonctions du système. Le système peut être pris au sens large, il ne concerne pas uniquement le système technique, mais peut aussi englober les hommes qui utilisent et maintiennent le système technique (Medina-Oliva, 2011).

Pour qu'une fonction soit correctement réalisée, il est nécessaire de lui fournir un ensemble de « flux » liés à son environnement : condition de fonctionnement, support de fonctionnement, énergie, commandes etc. Ces flux peuvent par exemple être typés, comme l'a proposé (Léger, 1999), sous la forme suivante :

- DF (Devoir Faire) : c'est un flux porteur des objets finalisant ou finalisés du système de nature informationnelle, matérielle ou énergétique.
- PF (Pouvoir Faire) : c'est un flux porteur des objets ressources du système. Il est de nature matérielle, énergétique, humaine ou logicielle.
- SF (Savoir Faire) : c'est un flux porteur des objets informant le système. Ce sont des informations transactionnelles.
- VF (Vouloir Faire) : c'est un flux porteur des objets stimulant un événement sur le système. Ce sont des informations événementielles.

Plusieurs flux DF, PF, SF et VF peuvent contribuer à la réalisation d'une fonction. Le motif générique d'une fonction est alors présenté (Figure 60). Pour chaque fonction définie dans l'analyse fonctionnelle, une brique de modélisation par RB peut être spécifiée.

Un nœud du RB est associé à chaque flux. A partir du motif générique d'une fonction nous définissons le motif générique du RB qui lui est associé (Figure 61). Ce RB permet de modéliser l'impact sur les flux sortants de la fonction de l'environnement décrit par les flux entrants. Les variables peuvent être multi-états et les relations de dépendance entre les variables peuvent être définies par des lois de probabilités conditionnelles quelconques. L'analyse AMDEC permet de définir les modalités des variables représentant les composants en relation avec les défaillances et les différents états des composants ainsi que les flux de sortie des fonctions avec leurs modes de fonctionnement et de dysfonctionnement. L'analyse HAZOP permet de définir les modalités des variables modélisant les flux de produit ou de matière. Un RB est le formalisme support qui permet d'implémenter le modèle.

Les relations entre les variables ne sont pas nécessairement déterministes et chaque variable parent peut produire un effet sur la variable enfant avec des probabilités différentes. L'opérateur OU-Bruité (Noisy-OR) (Pearl, 1988; Cozman, 2004) est très intéressant pour spécifier la loi de probabilité conditionnelle des variables modélisant les flux de sortie. Cet opérateur OU-Bruité est un operateur fournissant une aide pour la construction et la modélisation par un RB de variables dépendant de plusieurs variables parents. Il permet de construire la TPC en spécifiant pour une variable la probabilité d'influence de chacun de ses parents (Koller et Friedman, 2009, page 175). Le choix d'une telle structure, qui est une extension de la structure logique OU, permet de prendre en compte les facteurs d'influence entre les flux d'entrée et le flux de sortie pour la modélisation d'une fonction. Le choix de cette logique permet ainsi de propager de l'incertain sur les conséquences de la combinaison d'événements initiateurs (les flux entrant). Notons également que cette structure présente l'avantage de réduire l'effort de quantification des TPC en ne nécessitant que la connaissance de n paramètres pour remplir entièrement la TPC d'une variable à n parents (au lieu de $2n$) (Fallet 2012, page 31).

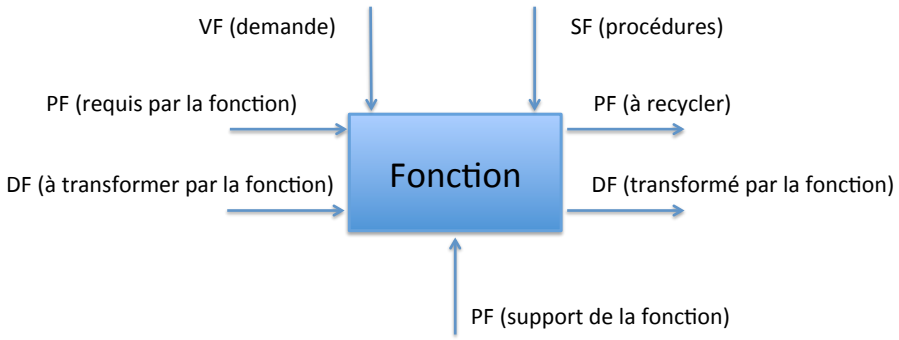


Figure 60 : Définition générique d'une fonction et de ses flux

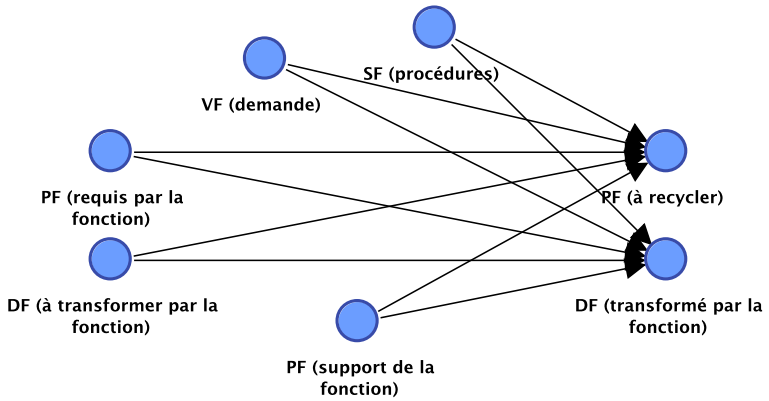


Figure 61 : Motif générique du RB modèle d'une fonction

Tableau 54

Flux entrant de la fonction	Variable	Flux sortant de la fonction
PF (V1, V2, V3) ; DF (fluide à transférer) ; VF (commande)	L	DF (L)

PF (V1) ; DF (fluide à transférer) ; VF (commande)	L_1	DF (L1)
DF (L1) ; PF (V2) ; VF (commande)	L_2	DF (L2)
DF (L1) ; PF (V3) ; VF (commande)	L_3	DF (L3)
PF (V1, V2, V3) ; DF (fluide à transférer) ; VF (commande)	I	DF (I)
PF (V1) ; DF (fluide à transférer) ; VF (commande)	I_1	DF (I1)
PF (V2) ; DF (fluide à transférer) ; VF (commande)	I_2	DF (I2)
DF (I2) ; PF (V3) ; VF (commande)	I_3	DF (I3)

Pour illustrer le principe de modélisation nous appliquons cette démarche pour structurer le modèle du système Figure 2. Une analyse fonctionnelle est donnée (Figure 62, Figure 63, Figure 64 et Figure 65). A partir de la modélisation fonctionnelle, les variables x_1, x_2, x_3 sont associées respectivement aux flux PF (V1), PF (V2), PF (V3), représentant les composants du système. La variable y est associée au flux DF (fluide transféré) et représente la finalité du système. Pour chaque fonction une variable est définie (Tableau 54) représentant sont flux de sortie dépendant des flux d'entrée de la fonction.

Pour être conforme aux analyses précédentes, les flux de commande VF (commande) et de matière consommée DF (fluide à transférer) ne sont pas représentés dans la modélisation par RB. La structure du RB (Figure 66) est construite simplement en reliant les flux tels que l'analyse fonctionnelle le définit. L'analyse fonctionnelle définit la fonction « Laisser passer 2 » avec le flux de sortie DF (L2) qui est représenté par L_2 dans le RB. Les flux d'entrée de la fonction sont DF (L1), PF (V2) (et VF (commande) non modélisé). Les parents de la variable L_2 sont donc représentés dans le RB par L_1 et x_2. Nous procédons de la même manière pour construire le modèle en connectant toutes les variables représentant les fonctions du système modélisées lors de l'analyse fonctionnelle. Le modèle obtenu est équivalent aux modèles précédents, mais cette fois, il repose sur une démarche de construction structurée à partir de la vue fonctionnelle et dysfonctionnelle du système.

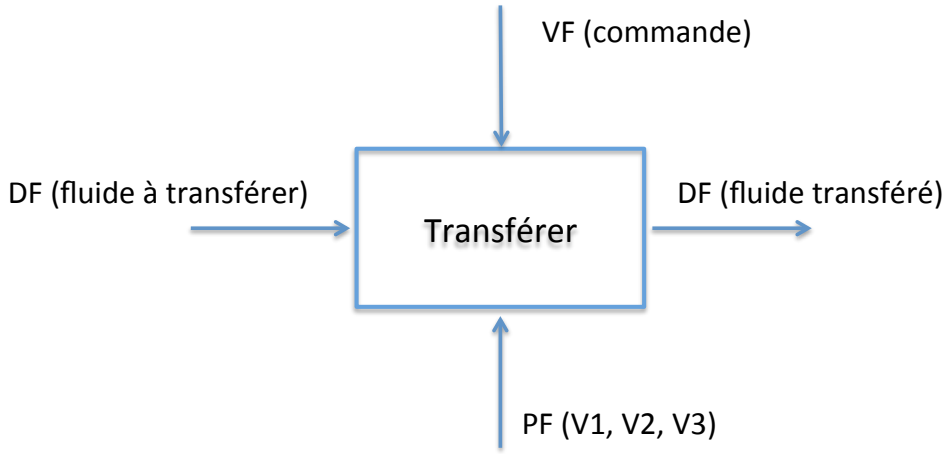


Figure 62 : Modèle fonctionnel du système de transfert de fluide

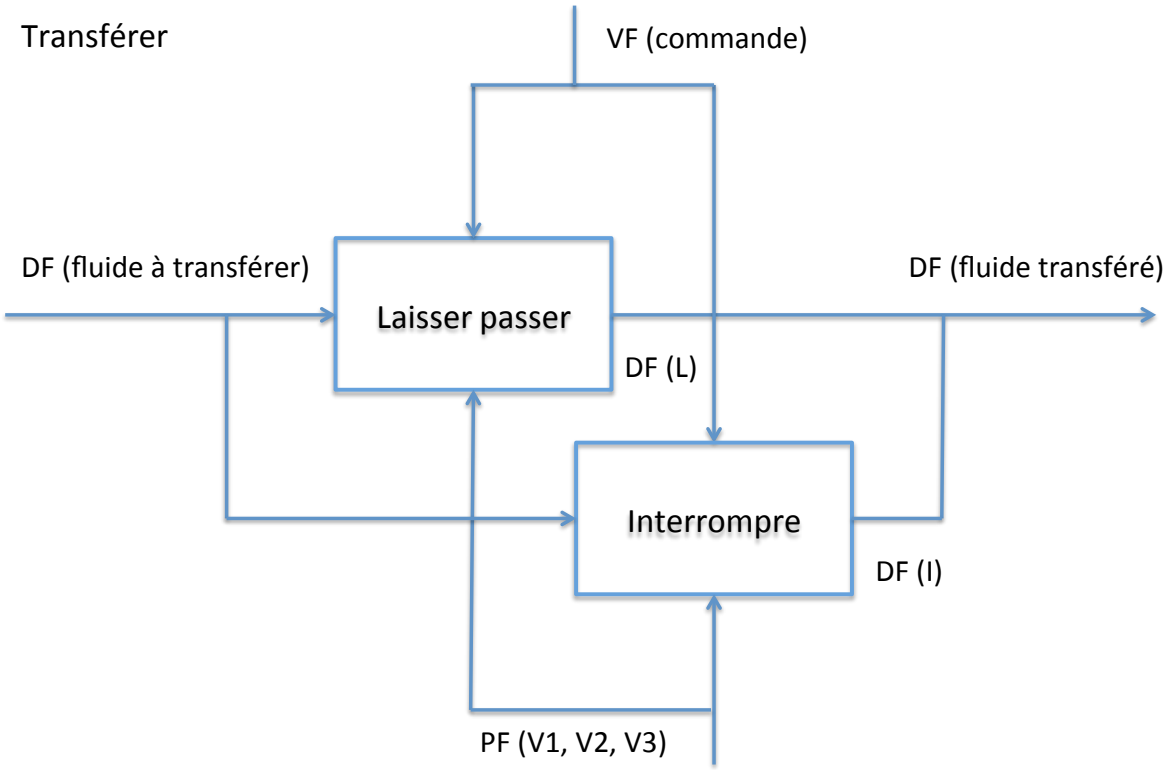


Figure 63 : Modèle fonctionnel du système (fonction Transférer)

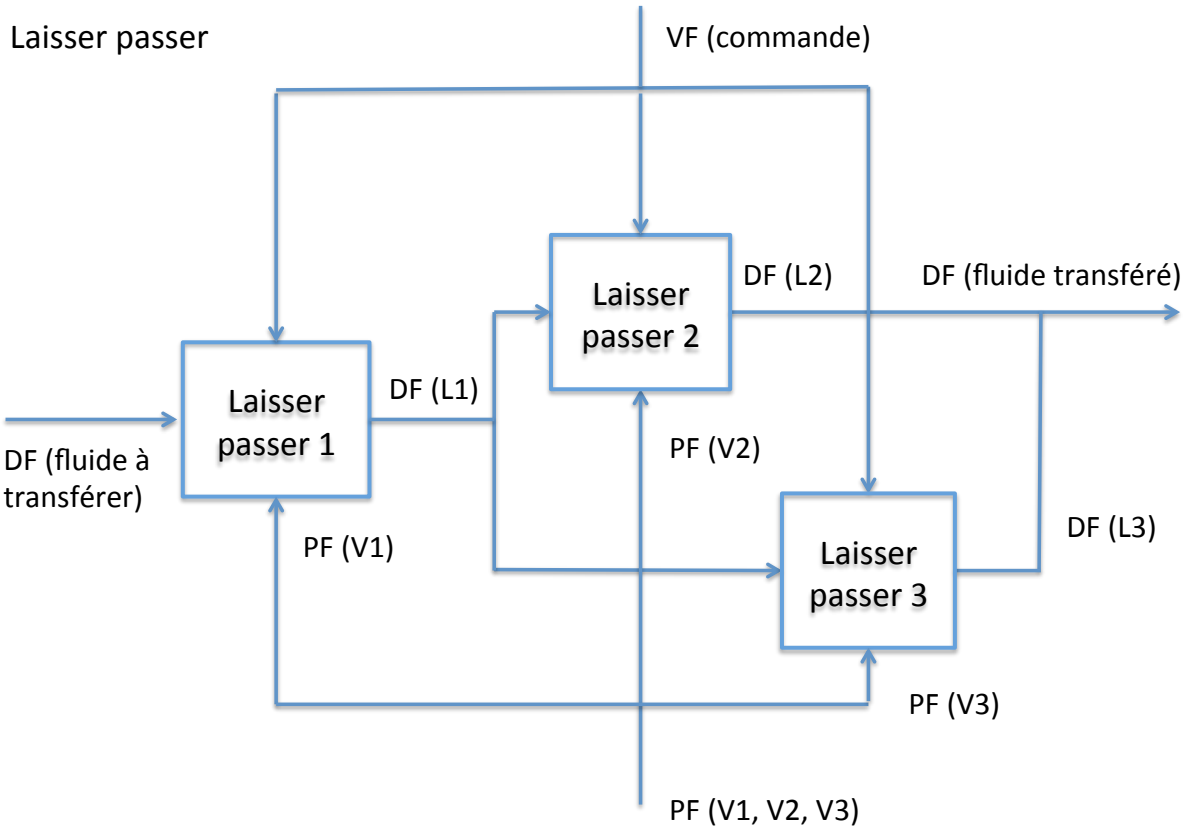


Figure 64 : Modèle fonctionnel du système (fonction Laisser Passer)

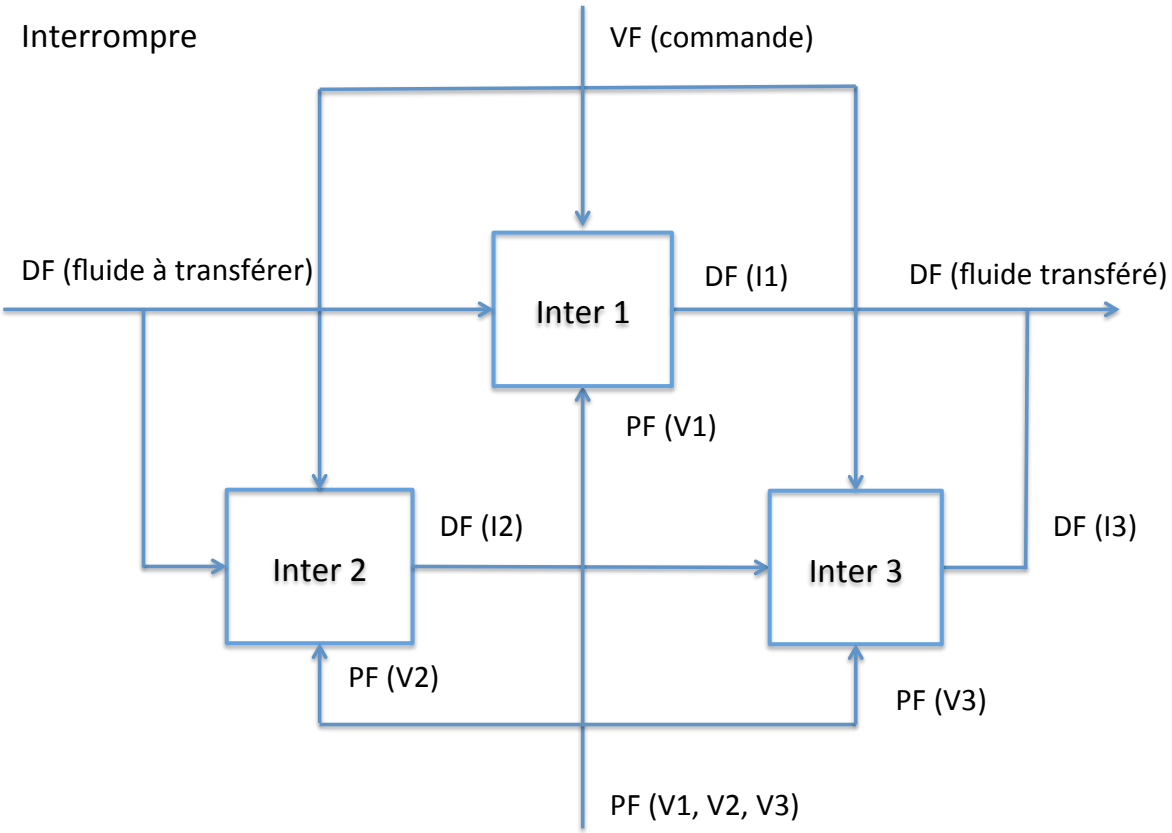


Figure 65 : Modèle fonctionnel du système (fonction Interrompre)

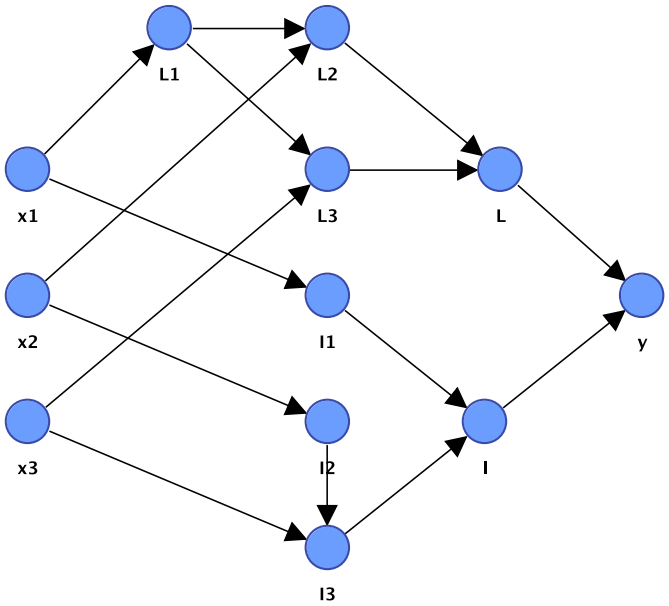


Figure 66 : RB structuré à partir de l'analyse fonctionnelle

Par inférence dans le RB avec les distributions de probabilité sur les variables x_i définies (Tableau 25, Tableau 26, Tableau 27), nous calculons la distribution de y. Le résultat est conforme à la distribution éq.(24). Les distributions des variables représentant le découpage fonctionnel du système L, L_1, L_2, L_3, I, I_1, I_2 et I_3 (Tableau 54) sont également calculées.

Tableau 55

y	
0	0,345721859
1	0,654278141

L	
0	0,681027695
1	0,318972305

L_1	
0	0,77218
1	0,22782

L_2	
0	0,524348829
1	0,475651171

L_3	
0	0,488172196
1	0,511827804

I	
0	0,664694164
1	0,335305836

I_1	
0	0,54437
1	0,45563

I_2	
0	0,51843
1	0,48157

I_3	
0	0,264083058
1	0,735916942

La probabilité $\mathbb{P}(L = 0) = 0{,}681027695$ (Tableau 55) correspond bien à la probabilité que le système laisse passer le fluide que nous avions calculé à l'éq. (32) pour le cas de l'analyse booléenne à partir des liens minimaux. $\mathbb{P}(L = 1) = 0{,}335305836$ correspond à la valeur calculée à partir des coupes minimales éq. (35) et est conforme à la valeur obtenue par le calcul dans l'arbre de défaillance (36). La démarche de construction du RB présentée généralise donc bien les autres méthodes de modélisation au cas multi-état.

E Modèle stochastique de fiabilité des composants

Pour modéliser l'évolution temporelle de l'incertitude sur l'état d'un composant, en sûreté de fonctionnement, un modèle du comportement de processus est représenté comme une variable aléatoire discrète qui prend ses valeurs dans un espace fini d'état correspondant aux états possibles de fonctionnement ou de panne du composant. Il est alors possible de poser plusieurs hypothèses sur les caractéristiques du processus qui conduisent à des modèles des complexités variables.

E.1 Processus de Markov invariable dans le temps

La fiabilité d'un composant peut être modélisée par une Chaîne de Markov (CM). Cette méthode de modélisation est très classique et conduit à une représentation graphique du modèle correspondant à un système d'équations différentielles (Ansell et Phillips, 1994, p. 124 ; *Cocozza-Thivent, 1997, p. 283-294*).

Soit $x_i^{(k)}$ une variable aléatoire discrète représentant un composant avec un nombre d'états fini et mutuellement exclusif :

$x_i^{(k)} = 0$ si le composant i est dans l'état de fonctionnement normal,
$x_i^{(k)} = \{1 \dots (l_i - 1)\}$ si le composant i est dans un état de fonctionnement dégradé, (43)
$x_i^{(k)} = \{l_i \dots n_i\}$ si le composant i est dans un état de dysfonctionnement.

Les états $\{1 \dots (l_i - 1)\}$ sont des états de fonctionnement dégradés, c'est à dire que le composant n'est pas dans l'état de fonctionnement normal, il est altéré ou dégradé, mais il peut toujours être utilisé et réalise sa mission. Les états $\{l_i \dots n_i\}$ sont des états de panne du composant qui peuvent avoir des conséquences différentes sur le système se traduisant par exemple par différents modes de défaillance (définis par exemple à partir d'une analyse AMDEC).

Le vecteur $\mathbb{P}\left(x_i^{(k)}\right)$ décrit la distribution de probabilité sur les états du composant. Pour une CM, ce vecteur est calculé pour chaque instant k :

$$\mathbb{P}\left(x_i^{(k)}\right) = \left[\mathbb{P}\left(x_i^{(k)} = 0\right) \dots \ \mathbb{P}\left(x_i^{(k)} = l_i\right) \ \dots \ \mathbb{P}\left(x_i^{(k)} = n_i\right)\right], \quad (44)$$

avec $\sum_{e=0}^{n_i} \mathbb{P}\left(x_i^{(k)} = e\right) = 1$.

La matrice $\mathcal{P}$ définit les transitions entre les états du composant. Une CM à temps discret est utilisée pour modéliser le processus à partir des taux de défaillances du composant.

$$\mathcal{P} = \begin{bmatrix} p_{00} & \cdots & p_{0n_i} \\ \cdots & & \cdots \\ p_{n_i 0} & \cdots & p_{n_i n_i} \end{bmatrix} \tag{45}$$

Le paramètre $p_{ee'}$ est la probabilité de transition entre l'état e et e' durant l'intervalle de temps entre k et $k+1$. Par convention et comme les processus étudiés en sûreté de fonctionnement sont très lent cet intervalle de temps est choisi égal à 1 heure pour la discrétisation.
La probabilité de transition $p_{ee'}$ peut être vue comme une probabilité conditionnelle :

$$p_{ee'} = \mathbb{P}\left(x_i^{(k+1)} = e' \middle| x_i^{(k)} = e\right) \tag{46}$$

Pour une CM homogène, les paramètres $p_{ee'}$ de la matrice $\mathcal{P}$ sont constants.

Le calcul du vecteur de distribution de probabilité $\mathbb{P}\left(x_i^{(k)}\right)$ est fait soit de manière analytique par résolution du système d'équations différentielles sous-jacent, ou après discrétisation du processus continu par un calcul itératif donnée par l'équation de Chapman-Kolmogorov. Les états fonctionnants $e \in \{0 \dots (l_i - 1)\}$ permettent de calculer la fiabilité du composant :

$$R_i^{(k)} = \sum_{e=0}^{l_i - 1} \mathbb{P}\left(x_i^{(k)} = e\right) \tag{47}$$

Le système est lui aussi défini par une variable multi-état en relation avec les scénarios de fonctionnement et les scénarios de dysfonctionnement du système. Le système est modélisé par une variable y qui prend les valeurs suivantes :

$y = 0$ correspond au fonctionnement normal (bon fonctionnement),
$y = \{1 \dots (l-1)\}$ correspond à un état de fonctionnement dégradé, (48)
$y = \{l \dots n\}$ correspond à des états de dysfonctionnement du système.

La fiabilité du système est calculée :

$$R^{(k)} = \sum_{e=0}^{l-1} \mathbb{P}\left(y^{(k)} = e\right) \tag{49}$$

La complexité de la structure de la Chaîne de Markov ainsi que le nombre de paramètres augmentent rapidement en fonction du nombre d'états du système. En effet, l'espace d'état décrivant le système est défini sur le produit cartésien des états des composants.

Exemple :
La probabilité de fonctionnement d'une vanne i est donnée par une Chaîne de Markov à 3 états {0, 1, 2} correspondant respectivement aux états $\{Ok, Pf, Po\}$ (Figure 67).

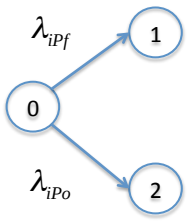


Figure 67. Chaîne de Markov d'un composant à trois états.

En utilisant les probabilités de défaillance $\lambda_{1Pf} = 1 \cdot 10^{-3}$ et $\lambda_{1Po} = 2 \cdot 10^{-3}$, le modèle de la vanne 1 par un RBD est présenté (Figure 68), l'inférence permet de calculer sur 1000h la distribution $\mathbb{P}\left(x_1^{(k)}\right)$.

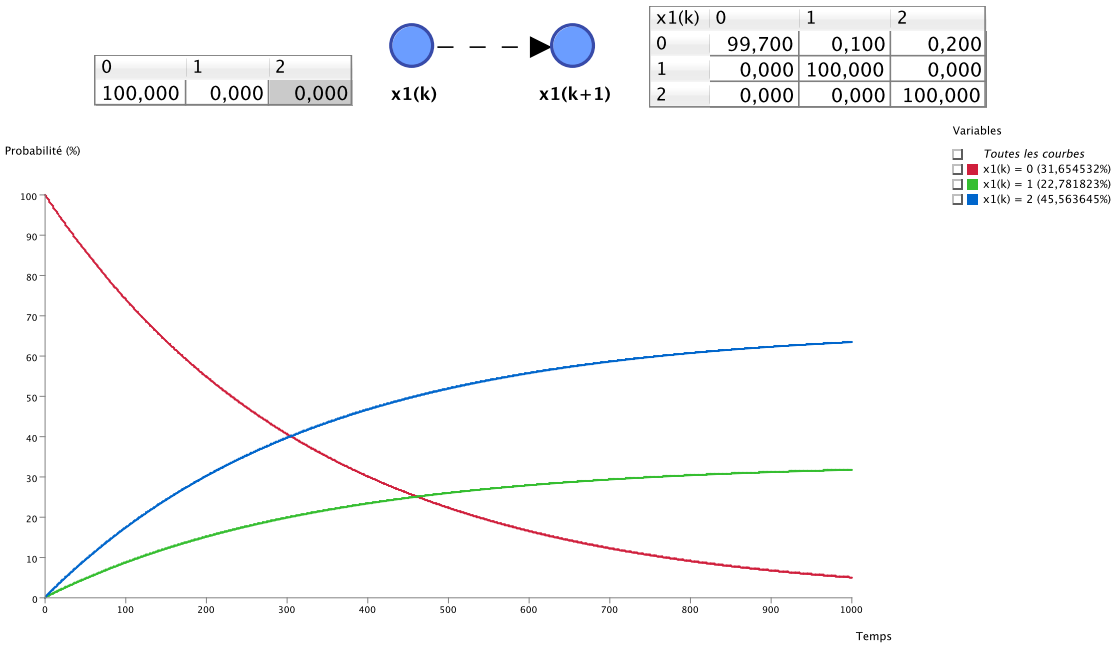


Figure 68 : Modèle RB Dynamique sur deux tranches de temps de la Vanne 1

E.2 Processus à paramètre variable dans le temps

L'hypothèse principale de modélisation par une Chaîne de Markov (CM) est que le temps de séjour dans chaque état est défini par une loi exponentielle. Selon cette hypothèse, les probabilités de transition entre les états sont considérées comme indépendantes du temps conduisant à l'analyse

de systèmes ayant des taux de défaillance constants. Malheureusement, la distribution exponentielle est bien souvent insuffisante car dans la majorité des problèmes d'ingénieries, elle ne reflète pas le fait que la plupart des composants subissent des détériorations en raison de leur utilisation, de leur usure ou de leur âge. La fonction de densité de probabilité de la distribution des temps de défaillance est alors modélisée par une distribution continue comme dans le cas d'une distribution Gamma, Weibull ou Normale. Pour modéliser ce type de comportement, une généralisation du processus de Markov appelé processus semi-Markovien (SMP) est introduite (Gertsbakh (2000) p 117 et Limnios (2001)). Les probabilités de transition entre les états ne sont pas constantes mais varient avec le temps. La matrice $\mathcal{P}$ devient dépendante du temps et la CM n'est plus homogène.

$$\mathcal{P}(k) = \begin{bmatrix} p_{00}(k) & \dots & p_{0n_i}(k) \\ \dots & & \dots \\ p_{n_i0}(k) & \dots & p_{n_in_i}(k) \end{bmatrix} \tag{50}$$

A partir des lois de dégradations, la transition entre états de fonctionnement et états de panne est défini par une équation en fonction du temps.

E.3 Hypothèse de processus non observables

Dans les procédés stochastiques de la section précédente la variable $x_i^{(k)}$ est supposée observable. En pratique, cela n'est pas la réalité car les changements d'états d'un composant ne sont observés que s'ils conduisent à une variation de la fonction du composant. Pour modéliser un tel processus (avec des états non observables ou pour lesquels l'observation de $x_i^{(k)}$ en temps réel est trop coûteuse), une variable $z_i^{(k)}$ est utilisée pour caractériser le niveau de détérioration et les états de $x_i^{(k)}$ sont vue comme un processus stochastique caché. Soit $z_i^{(k)}$ une variable aléatoire discrète qui définit les modes de défaillances et de fonctionnements d'un composant, le changement de l'état du composant $x_i^{(k)}$, n'est observé qu'à travers une altération de la fonction du composent c'est à dire les changements d'état de la variable $z_i^{(k)}$. Dans ce cas, la distribution de $z_i^{(k)}$ est définie conditionnellement à $x_i^{(k)}$ par $\mathbb{P}\left(z_i^{(k)} \middle| x_i^{(k)}\right)$. Le composant $x_i^{(k)}$ est alors modélisé comme un Modèle de Markov Caché noté HMM pour « Hidden Markov Model ». Habituellement utilisé en reconnaissance de la parole (Rabinet, 1989) ou l'analyse financière, un HMM est un processus doublement stochastique avec un processus stochastique sous-jacent non observable. Le processus $x_i^{(k)}$ est observé à travers un autre ensemble de processus stochastique $z_i^{(k)}$ qui produisent la séquence d'observations. L'état de $x_i^{(k)}$ est alors déduit de l'observation d'une séquence de $z_i^{(k)}$.

E.4 Hypothèse de processus sous contrainte exogène

Le temps est souvent considéré comme le facteur qui conditionne la fiabilité du composent. Cela peut s'avérer insuffisant (Singpurwalla, 1995), les conditions d'exploitation et l'environnement (par exemple humidité, température) peuvent également altérer la fiabilité d'un composant. Tous ces facteurs qui peuvent impacter la fiabilité d'un composant sont appelés Co-variables ou variables explicatives (Bagdonavicius et Nikulin, 2001). La fiabilité d'un composant peut être modélisée de manière plus précise en prenant en compte les effets des Co-variables (Cox, 1955). Pour tenir compte des événements exogènes, nous pouvons définir plusieurs modèles par CM qui représentent chaque situation en fonction du contexte d'exploitation du composant.

Un Modèle de Markov Commuté noté MSM pour « Markov Switching Model » peut être introduit pour modéliser ce type de processus stochastique intégrant l'impact d'événements exogènes qui conditionnent le passage d'une CM à une autre. Ces modèles sont également considérés comme des CM conditionnelles où les probabilités de transition sont conditionnelles à une variable exogène. Les modèles MSM sont non-stationnaires à cause des changements brutaux dans les paramètres du modèle (Bengio 1999 pp 147). Un MSM représente la distribution conditionnelle $\mathbb{P}\left(x_i^{(k)}\middle|u_i^{(k)}\right)$ compte tenu de la séquence d'état de l'entrée $\left[u_i^{(0)}, u_i^{(1)}, \dots u_i^{(k)}\right]$ où $u_i^{(k)}$ représente l'état de la contrainte exogène. La simulation d'un modèle de Markov commuté est basée sur la commutation et la procédure d'initialisation de la CM en fonction de l'état de la variable exogène. Il est très difficile d'obtenir la solution analytique de ce type de système différentiel hybride.
Enfin, si l'état de la variable exogène $u_i^{(k)}$ n'est pas connu, mais une séquence de distribution de probabilité permet de décrire ses états, le processus stochastique est formalisé sous la forme d'un processus de Markov caché conditionné par un séquence d'entrée $u_i^{(k)}$ que nous notons (IOHMM) pour « Input-Output Hidden Markov Model ». La variable observable exogène $u_i^{(k)}$ est vue comme une entrée, et l'impact du processus caché vue à travers les modes de défaillances est défini comme une sorties $z_i^{(k)}$. Les variables $u_i^{(k)}$ et $z_i^{(k)}$ induisent plusieurs comportements du processus non observable (caché) $x_i^{(k)}$ décrivant la dégradation du composant. Pour modéliser ce processus stochastique complexe $\mathbb{P}\left(z_i^{(k)}\middle|x_i^{(k)}, u_i^{(k)}\right)$, le formalisme des (IOHMM) est bien adapté (Bengio 1999 pp 145).

E.5 Conclusion

Les modèles CM, HMM, MSM ou IOHMM sont des modèles adaptées pour modéliser la fiabilité d'un composant ou d'un système complexe de faible dimension. La résolution en temps discret des processus stochastiques complexes (non markovien homogène ou semi-markovienne) pour obtenir l'équation d'évolution n'est pas une tâche facile. Les solutions peuvent être obtenues analytiquement dans des cas spécifiques et simples, dans les autres cas il est nécessaire d'utiliser une méthode itérative après discrétisation.

Pour des applications à des cas industriels, l'explosion combinatoire des états rend ces méthodes difficilement exploitables. Cette formalisation fournit une représentation synthétique des systèmes complexes composées des processus précédemment mentionnés car il permet de factoriser les processus indépendant.

Avis des Parrains Scientifiques

CENTRE DE RECHERCHE EN AUTOMATIQUE DE NANCY

Avis sur la demande présentée par Philippe Weber en vue de s'inscrire à l'Habilitation à Diriger des Recherches à l'Université de Lorraine

Avis établi par ses deux parrains – Prof. Benoît IUNG et Prof. Didier THEILLIOL

Du CRAN UMR CNRS 7039 - Université de Lorraine

Philippe Weber, âgé de 43 ans, est Maître de Conférences, 61ème section, en poste à l'Université de Lorraine. Il exerce ses activités de recherche au sein du CRAN (Centre de Recherche en Automatique de Nancy ; UMR CNRS 7039) et ses activités statutaires d'enseignement à l'ESSTIN (Ecole Supérieure des Sciences et Technologies de l'Ingénieur de Nancy).

Depuis septembre 2000, Philippe Weber occupe ce poste de Maître de Conférences sur un profil d'emploi publié au concours n°61MCF07775 avec l'intitulé « maintenance industrielle et sûreté de fonctionnement des systèmes de production ». Cette thématique est centrale à la fois au cursus universitaire de M. Weber mais aussi à ses activités passées et actuelles qu'elles soient d'enseignement ou de recherche. En effet, relativement à sa formation, après un parcours EEA (DEUG, licence et maîtrise) suivi à l'Université Henri Poincaré Nancy I, Philippe Weber a obtenu en 1995 un DEA en Automatique et Traitement Numérique du Signal – option diagnostic (mention assez bien) toujours dans cette même université puis un doctorat, en 1999, en Automatique et Productique de l'INP de Grenoble sur un sujet d'estimation paramétrique appliquée au diagnostic des procédés (sous la direction du Prof. Sylviane Gentil). Ce parcours de formation lui a permis ainsi de revendiquer très clairement lors de sa qualification aux fonctions de Maître de Conférences de réelles compétences scientifiques en diagnostic-sûreté de fonctionnement.

En ce sens depuis sa nomination, sur le volet pédagogie, P. Weber assure des enseignements et des responsabilités majoritairement sur les thématiques «maintenance, sûreté de fonctionnement, systèmes tolérants aux fautes, et risques». Pour participer plus fortement à l'offre de formation de l'ESSTIN, il a été responsable de l'option Maintenance Industrielle de 2004 à 2005 puis de 2008 à 2010 et assure aujourd'hui la responsabilité de l'option – Maintenance et Sûreté des Systèmes (MSS). A ces responsabilités sont aussi associées la définition des programmes pédagogiques en cohérence avec les attendus de la CTI et sa forte implication au niveau relation avec l'industrie (ex. suivi de projets industriels, responsabilité des stages). Ses enseignements se font majoritairement à l'ESSTIN (Bac + 1 à Bac + 5) avec une responsabilité de plusieurs UEs en sachant que certains de ces cours sont adaptés pour être dispensés au sein du M2 du master ISC, dans les UEs de recherche. Ce désir d'être acteur au sein du master ISC, est représentatif de la volonté de P. Weber de rapprocher autant que faire se peut son activité d'enseignement de son activité de recherche. En ce sens il a toujours cherché à être force de proposition dans les différents cursus de formation. Ainsi, P. Weber a su proposer et créer des UEs à partir des transferts de ses résultats scientifiques, par exemple en lien avec de nouveaux outils de modélisation comme les réseaux bayésiens, les réseaux de fonction de croyance ... et avec dynamisme, a récemment prôné une évolution des enseignements en

CRAN UMR 7039
CAMPUS SCIENCES - BP 70239 - 54506 Vandœuvre-lès-Nancy - Cedex
Tél. : + 33 (0)383684419 - Fax : + 33 (0)383684437
E-mail : cran-secretariat@univ-lorraine.fr - Web : www.cran.univ-lorraine.fr

maintenance pour intégrer la notion de développement durable (en cohérence avec le futur projet pédagogique de l'ESSTIN).

Concernant les activités de recherche, les travaux menés par P. Weber portent, de manière synthétique, sur la formalisation de méthodes de modélisation graphique probabiliste telle que les réseaux bayésiens (RB) pour résoudre différentes problématiques liés à la sûreté de fonctionnement-maintenance des systèmes complexes. Ces travaux se positionnement logiquement dans différents comités techniques de fédérations scientifiques IFAC, IEEE ou ESRA à l'international, et des groupes de travail du GdR MACS et de l'IMdR au national. Cette recherche s'inscrit majoritairement dans une recherche méthodologie et technologique en visant un équilibre entre le développement d'actions à caractère « fondamental » (ex. extension mathématique de l'outil RB) et l'ouverture à des problèmes industriels. Ainsi à juste titre, P. Weber revendique fortement une recherche se nourrissant de verrous scientifiques émergents de problématiques industrielles complexes. Il a ainsi des relations pérennes avec des industriels comme EDF, RATP, SNCF (ex. 3 thèses CIFRE réalisées), a participé à plusieurs projets Européens (3) et à 11 projets nationaux (dont 2 conséquents en tant que porteurs), et a un partenariat très privilégié avec la société BAYESIA développant l'outil BayesiaLab support aux RB. Ces travaux ont donc pour objet de faire le lien entre les formalismes mathématiques de modélisation et leurs utilisations par des industriels. L'originalité de ces travaux est construite sur cette dualité pour laquelle les contributions de P. Weber, principalement sous la forme de modèles ou d'extension des principes de l'outil RB, adressent la prise en compte des incertitudes, la propagation de ces incertitudes, l'évaluation conjointe de risques multisectoriels, l'évaluation de stratégie, la mesure d'exigences d'allocation etc.

Ces contributions se structurent sur deux axes principaux:

- La modélisation en maîtrise des risques, en maintenance et en fiabilité pour des systèmes sociotechniques complexes ;
- L'intégration des connaissances de fiabilité dans la commande et le diagnostic des systèmes.

Ce double volet recherche justifie l'appartenance, au sein du CRAN, de P. Weber à 2 départements et à un projet de chaque département que sont : dépt. ISET (Ingénierie des Systèmes Eco-techniques) – projet « Sûreté de Fonctionnement Système (SdFS) » et dépt. CID (Contrôle, Identification, Diagnostic) projet « Co-conception de Systèmes Dynamiques sûrs de Fonctionnement (CSDF) ». Cette double appartenance est revendiquée aussi dans le projet de recherche pour développer des travaux en continuité des deux axes d'objectifs précédemment cités.

Sur la période 2002-2014, les contributions scientifiques ont été majoritairement faites à l'initiative de P. Weber (en lien avec d'autres chercheurs du CRAN) ou dans le cadre de thèses. En effet P. Weber a participé au co-encadrement/co-direction (avec Pr. D. Theilliol ou Pr. B. Iung) de 7 thèses dont une actuellement en cours et de 7 masters. Il est important de souligner que les encadrements de thèse ont tous donné lieu à des publications. Au global d'un point de vue production scientifique quantitative, P. Weber fait état de 20 publications dans des revues internationales d'1 revue nationale, de 6 participations à des ouvrages, d' 1 conférence invitée et de 85 conférences internationales ou nationales. D'un point de vue qualitatif, la majorité des journaux ciblés par P. Weber sont des journaux reconnus de la communauté sûreté – maintenance avec des facteurs

UNIVERSITÉ DE LORRAINE
CRAN UMR 7039
CAMPUS SCIENCES - BP 70239 - 54506 Vandœuvre-lès-Nancy - Cedex
Tél. : + 33 (0)383684419 - Fax : + 33 (0)383684437
E-mail : cran-secretariat@univ-lorraine.fr - Web : www.cran.univ-lorraine.fr

d'impact conséquents. De plus certaines publications en revue sont citées plus de 100 fois (référence Google scholar citations). Ce bilan est tout à fait conséquent en quantité et en qualité pour un candidat à l'HDR.

D'un point de vue rayonnement, P. Weber a été sollicité pour 2 sessions plénières, la participation à 2 jurys de thèse, l'expertise de nombreux papiers soumis en revue, la participation à plusieurs comités de programme (ex. Qualita, Lambda Mu) et au comité d'organisation de Qualita'03, Qualita'2015. Il a organisé aussi 4 sessions invitées, un séminaire international au Mexique (thème BN applications in dependability), et est membre du groupe d'intérêt « Technology and Process of Care in Emergency Care » de l'EuSEM. Il revendique de nombreuses relations avec des Universités à l'international comme celles de Barcelone, de Western Ontario, du Piémont ou au national comme avec les laboratoires du Gipsa-Lab, du Gscop, de l'IRSTEA... L'élément majeur du rayonnement est la création et l'animation avec C. Simon au sein de l'IMdR du GTR « Réseaux probabilistes appliqués à la maîtrise des risques et à la sûreté de fonctionnement ». Ce groupe est actif depuis 2013 avec une quinzaine de participants.

Sur le plan des responsabilités collectives en recherche, il convient de citer l'élection de P. Weber au conseil du laboratoire CRAN (2008-2012, 2013-2017), sa participation au bureau de ce conseil (08-12), à la commission information scientifique et technique du CRAN (2013-2017), à différentes commissions de spécialistes ...

En conclusion, Philippe Weber présente un dossier à l'inscription à l'HDR de grande qualité et très bien équilibré puisque l'activité d'enseignement vient se nourrir des résultats de la recherche. L'encadrement doctoral est avéré avec une production scientifique importante dans des journaux à fort impact. Cette activité de recherche est déjà reconnue, entre autres, à travers les collaborations établies avec des laboratoires au niveau international et national mais aussi l'animation scientifique du GTR de l'IMdR. Ce rayonnement confère une réelle crédibilité et originalité à la recherche menée. De plus, la relation de P. Weber avec le monde industriel est incontestable de par le financement de certaines thèses CIFRE, l'octroi de contrats et la participation à des projets Européens. Ce triple constat (encadrement, résultats, impact industriel) légitime les capacités de P. Weber à mener une recherche voire une équipe de recherche à la fois en regard de l'aspect scientifique en référence au projet proposé dans son manuscrit, des publications attendues, des impacts sociétaux et aussi des moyens à déployer. Enfin, en termes de responsabilités pédagogiques, P. Weber a pris en charge l'option de l'ESSTIN se rattachant aux thèmes de sa recherche ce qui lui permet de satisfaire à l'ensemble des attendus de sa fonction d'enseignant/chercheur.

En conséquence sur la base de ces conclusions, nous donnons, **sans réserve, un avis très favorable** à sa demande d'inscription à l'Habilitation à Diriger des Recherches de l'Université de Lorraine.

Fait à Nancy le 15/11/2014

Pr. Benoît IUNG

Pr. Didier THEILLIOL

UNIVERSITÉ DE LORRAINE

CRAN UMR 7039
CAMPUS SCIENCES - BP 70239 - 54506 Vandœuvre-lès-Nancy - Cedex
Tél. : + 33 (0)383684419 - Fax : + 33 (0)383684437
E-mail : cran-secretariat@univ-lorraine.fr - Web : www.cran.univ-lorraine.fr

Avis des Rapporteurs

gipsa-lab

Rapport sur le mémoire présenté par M. Philippe Weber
pour l'obtention de l'Habilitation à Diriger des Recherches de l'Université de Lorraine,
établi par Christophe Bérenguer, professeur à l'Institut Polytechnique de Grenoble

Parcours du candidat

Philippe Weber, âgé de 44 ans, a rejoint l'Ecole Supérieure des Sciences et Technologies de l'Ingénieur de Nancy (ESSTIN, Université de Lorraine) en septembre 2000 en tant que Maître de Conférences après un cursus universitaire à l'Université Henri Poincaré - Nancy 1 (Maîtrise EEA en 1994, DEA ATNS en 1995) et à l'Institut National Polytechnique de Grenoble (Doctorat en Automatique et Productique, 1999). Il est chercheur au Centre de Recherche en Automatique de Nancy (CRAN), dans les départements Ingénierie des Systèmes Eco-Techniques (ISET) et Contrôle-Identification-Diagnostic (CID).

Activités de recherche

Les travaux de recherche de Philippe Weber portent sur le développement de méthodes de modélisation graphique probabiliste (Réseaux Bayésiens) et sur leur mise en œuvre pour la modélisation et la résolution de problème liés à la sûreté de fonctionnement des systèmes industriels. Philippe Weber s'intéresse ainsi principalement à deux grandes classes de problèmes :

- Modélisation en maîtrise des risques, en maintenance et en fiabilité pour des systèmes sociotechniques complexes
- Intégration des connaissances de fiabilité dans la commande et le diagnostic des systèmes automatisés

Ces travaux se positionnement bien à l'intersection des départements ISET et CID du CRAN. Philippe Weber a su apporter des contributions scientifiques significatives et originales sur ces deux thématiques, en s'appuyant sur des méthodes de modélisation probabiliste graphique dont il est devenu un spécialiste reconnu. Philippe Weber présente ses travaux de recherche dans le chapitre 3 de son mémoire d'HDR. Il y défend en premier lieu les réseaux bayésiens comme un outil modélisation bien adapté aux problèmes actuels en sûreté de fonctionnement, justifiant ainsi son choix d'en faire l'outil de base de ses contributions scientifiques et méthodologiques. La démarche structurée de construction d'un modèle de sûreté de fonctionnement à base de réseaux bayésiens est ensuite présentée dans le cadre de systèmes à composants binaires, puis pour des systèmes à composants multi-états. Philippe Weber propose également une comparaison des modèles ainsi obtenus avec des modèles plus classiques de sûreté de fonctionnement. Il illustre la mise en œuvre de la démarche de modélisation proposée sur un problème de maintien en conditions opérationnelles, nécessitant le développement d'un modèle modulaire et hiérarchique du système d'intérêt, du système de maintenance et de leurs interactions. La suite de ce chapitre est consacrée aux réseaux bayésiens dynamiques, ainsi qu'à leur intérêt et leurs limites actuelles pour la modélisation de la sûreté et de la fiabilité des systèmes, avec intégration de l'environnement et des contraintes d'exploitation. Les applications des modèles probabilistes développés par Philippe Weber ne se limitent pas à la maîtrise des risques, la maintenance ou le diagnostic : des travaux originaux faisant le lien entre fiabilité et commande des systèmes sont présentés à la fin du chapitre 3. La définition d'une stratégie de commande pour des systèmes sur-actionnés permettant une répartition optimale des efforts sur les actionneurs en préservant la fiabilité du système (en nominal ou en présence de défaillances) constitue sans doute une des propositions de recherche les plus originales et porteuse de perspectives.

L'ensemble des travaux présentés dans le chapitre 3 montre que Philippe Weber contribue de manière pertinente, personnelle et originale au développement de recherches à l'interface des disciplines "automatique", "fiabilité" et "productique" au sein du CRAN, et plus généralement au sein des communautés nationale et internationale concernées par ces sujets. Il est à noter enfin que Philippe Weber

GIPSA-lab
Campus universitaire
11 rue des Mathématiques - BP46
F-38402 GRENOBLE Cedex
Tél. +33 (0)4 76 82 62 56
Fax +33 (0)4 76 82 64 26

www.gipsa-lab.inpg.fr
prenom.nom@gipsa-lab.inpg.fr

Tutelles
Grenoble INP, CNRS,
UJF, Stendhal

a su construire lui-même ce positionnement scientifique original, en rupture avec ses travaux de thèse, ce qui montre son autonomie et sa maturité scientifiques.
Au-delà de son bilan d'activité, il défend également un projet de recherche original, ambitieux, crédible et convaincant, décliné en trois axes:

- Intégration des connaissances probabilistes dans la stratégie de commande des systèmes dynamiques
- Modélisation probabiliste en maîtrise des risques des systèmes socio-techniques et leurs impacts sur le développement durable
- Formalisation de modèles graphiques probabilistes en sûreté de fonctionnement pour de nouvelles classes de systèmes

Des collaborations, nationales et internationales, déjà bien identifiées ainsi qu'une volonté de développer une animation scientifique autour de ses thèmes de recherche, viennent renforcer le projet de recherche de Philippe Weber.

Activité de publication

L'ensemble des travaux de Philippe Weber a donné lieu à 17 publications en revues internationales reconnues (*Reliability Engineering & System Safety*, *Journal of Risk and Reliability*, *Engineering Applications of Artificial Intelligence*), toutes sur son activité de recherche postérieure au doctorat. Certaines de ses publications ont été reçues avec beaucoup d'intérêt par la communauté, comme en atteste leur taux de citation élevé. Cette activité de publication comporte également entre autres plusieurs contributions à des ouvrages collectifs et plus de 50 publications dans des conférences d'audience internationale reconnues (SAFEPROCESS, INCOM, IFAC WC,...). Il s'agit d'une production de très bon niveau en quantité et en qualité des revues choisies pour les publications. Les doctorants encadrés sont régulièrement associés aux publications en revues et en conférences internationales : près de la moitié des articles de revue sont co-signés avec des doctorants (les autres articles relèvent de travaux réalisés avec d'autres collaborateurs internes ou externes au CRAN).

Activités d'encadrement

Philippe Weber a co-encadré (à 50% avec soit D. Theilliol, soit B. Iung) 6 thèses de doctorat soutenues (de 2007 à 2012), et il co-encadre actuellement 1 thèse en cours à soutenir en 2016. Philippe Weber publie de façon soutenue avec ses doctorants encadrés et tous les docteurs formés sont insérés professionnellement dans l'industrie sur des postes en lien avec leurs travaux de recherche, ce qui contribue à témoigner de la qualité des travaux menés sous sa responsabilité et de son investissement dans l'encadrement. Philippe Weber a également encadré 7 stages de Master Recherche. Il a également été invité à participer comme examinateur à 3 jurys de thèse.

Responsabilités en recherche, animation scientifique, insertion dans la communauté, rayonnement

Philippe Weber est bien inséré dans les communautés scientifiques nationale et internationale dont relèvent ses activités scientifiques (IFAC Safeprocess, IEEE) : il participe ainsi à l'organisation de sessions spéciales en conférences ; il contribue à l'organisation de journées scientifiques ou de conférences nationales (participations à des comités scientifiques des conférences Qualita par exemple) ; il évalue des articles et des communications pour les principales revues et conférences internationales de son domaine ; il a été invité à plusieurs reprises à donner des conférences plénières ou des séminaires. Il ne fait aucun doute qu'il est un des experts qu'on sollicite sur les réseaux bayésiens et leur utilisation sur les problèmes de fiabilité et de maîtrise des risques.
Au niveau national, son activité d'animation se concentre sur la co-responsabilité du GTR "Réseaux probabilistes bayésiens appliqués à la maîtrise des risques et à la sûreté de fonctionnement" de l'Institut

GIPSA-lab
Campus universitaire
11 rue des Mathématiques - BP46
F-38402 GRENOBLE Cedex
Tél. +33 (0)4 76 82 62 56
Fax +33 (0)4 76 82 64 26

www.gipsa-lab.inpg.fr
prenom.nom@gipsa-lab.inpg.fr

Tutelles
Grenoble INP, CNRS,
UJF, Stendhal

pour la Maîtrise des Risques (IMdR), GTR qu'il a fondé en 2013 avec C. Simon. Au niveau local, Philippe Weber fait partie du conseil de son laboratoire depuis 2006.

Projets, contrats et collaborations industrielles.
Philippe Weber appuie ses recherches sur des contrats industriels et des projets collaboratifs évalués et financés, qui lui fournissent à la fois les moyens de développer ses travaux, un ancrage avec la réalité industrielle et des terrains de validation pour les méthodologies qu'il développe avec ses collaborateurs. Philippe Weber est ainsi impliqué dans des projets ou des contrats sans discontinuer depuis 2002 : participation à 3 projets de recherche européens (FP6 & FP7), porteur de 2 projets de recherche nationaux (1 projet industriel et 1 projet ANR), participation à 9 projets de recherche nationaux (CPER, IMdR, GIS 3SGS, ...). Au travers de ces projets, il entretient un partenariat industriel pérenne avec EDF, avec qui il a également monté 3 projets de thèse CIFRE.

Activités d'enseignement
Philippe Weber réalise la majeure partie de son activité d'enseignement en formation d'ingénieur à l'ESSTIN ; il intervient également en master "Ingénierie des Systèmes Complexes" de l'Université de Lorraine. Depuis sa nomination, dans une volonté de cohérence et de lien formation/recherche, il a progressivement pris la responsabilité des enseignements en maintenance, en sûreté de fonctionnement et en maîtrise des risques, jusqu'à assurer la responsabilité pédagogique de l'option "Maintenance et Sûreté de Systèmes". Philippe Weber assume ainsi de nombreuses responsabilités et assure des tâches collectives au sein de l'ESSTIN, où il développe une activité pédagogique en pleine cohérence avec ses activités de recherche.

Conclusion
Philippe Weber présente un excellent dossier de candidature à l'Habilitation à Diriger des Recherche, très équilibré sur l'ensemble des activités d'un enseignant-chercheur. Le bilan d'activité de Philippe Weber fait apparaître un enseignant-chercheur très dynamique et actif, innovant en recherche et en enseignement et investi dans son établissement. Philippe Weber peut faire valoir une expérience de recherche solide, des expériences d'encadrement réussies, validées par un très bon dossier de publications. Après une mobilité thématique et géographique post-doctorat, il a su mener ses activités de recherche en autonomie en développant une thématique de recherche originale dans son laboratoire d'accueil. Son parcours de recherche montre sans ambiguïté qu'il a toutes les capacités pour définir, réaliser et diriger des programmes de recherche, pour trouver les moyens de les mettre en œuvre dans le cadre de projets partenariaux et pour encadrer des chercheurs et former de jeunes chercheurs.
En conclusion, et pour toutes les raisons évoquées ci-dessus, je donne un avis très favorable, sans la moindre réserve, à la présentation des travaux de Philippe Weber en vue de l'obtention de l'Habilitation à Diriger des Recherches de l'Université de Lorraine.

Fait à Grenoble, le 22 mai 2015

Christophe Bérenguer
Professeur des Universités – 61ème section CNU
christophe.berenguer@grenoble-inp.fr

grenoble
images
parole
signal
automatique

GIPSA-lab
Campus universitaire
11 rue des Mathématiques - BP46
F-38402 GRENOBLE Cedex
Tél. +33 (0)4 76 82 62 56
Fax +33 (0)4 76 82 64 26

www.gipsa-lab.inpg.fr
prenom.nom@gipsa-lab.inpg.fr

Tutelles
Grenoble INP, CNRS,
UJF, Stendhal

CRIStAL
Centre de Recherche en Informatique, Signal et Automatique de Lille

Rapport sur le mémoire d'Habilitation à Diriger des Recherches présenté par **Philippe WEBER** rédigé par Vincent COCQUEMPOT, Professeur Université Lille1

Présentation générale du mémoire

Le document présenté par Philippe WEBER, Maître de Conférences à l'Ecole Supérieure des Sciences et Technologies de l'Ingénieur de Nancy (ESSTIN), Université de Lorraine, en vue de l'obtention de l'Habilitation à Diriger des Recherches, s'intitule « Modélisation graphique probabiliste pour la maîtrise des risques, la fiabilité et la synthèse de lois de commande des systèmes complexes».

Ce mémoire d'HDR est structuré en 4 chapitres. Le premier chapitre est un rapport d'activités (curriculum vitae étendu), le deuxième chapitre est une synthèse des activités d'enseignement et d'administration. Le chapitre 3 présente les activités de recherche que Philippe WEBER a développées au Centre de Recherche en Automatique de Nancy (CRAN UMR 7039). Enfin, le chapitre 4 décrit son projet de recherche.

Des annexes ont été ajoutées : la liste les documents pédagogiques réalisés est fournie, des précisions sur les méthodes et modèles utilisés dans le chapitre 3 sont apportées, 5 publications permettant de couvrir les travaux principaux réalisés sont fournies.

Impression générale

Le document fourni a été rédigé avec grand soin. Il permet de mettre en évidence l'équilibre que Philippe WEBER a su conserver tout au long de sa carrière d'enseignant-chercheur entre les activités d'enseignement, de recherche et d'administration. Il montre la qualité scientifique du candidat, l'originalité des recherches menées, son expertise, sa capacité de synthèse et le recul qu'il a acquis sur sa thématique de recherche, en lien constant avec les problématiques industrielles.

Activités d'enseignant-chercheur

Activités pédagogiques

Après un cursus universitaire (DUT GEII, DEUG, Licence et Maîtrise EEA, DEA *Automatique et Traitement Numérique du Signal, option diagnostic*) suivi à l'Université Henri Poincaré Nancy 1, Monsieur WEBER a préparé une thèse de doctorat à l'Institut Polytechnique de Grenoble, sous la direction de Mme Sylviane GENTIL. Il a soutenu cette thèse intitulée « Estimation paramétrique appliquée au diagnostic des procédés » le 26 octobre 1999.

Monsieur WEBER a ensuite obtenu un poste d'ATER à l'ESSTIN, Nancy Université, puis a été recruté comme Maître de Conférences à l'ESSTIN en 2000.

Depuis sa nomination en 2000, Philippe WEBER s'implique et s'investit dans son établissement d'affectation. Il a ainsi assuré un certain nombre de responsabilités pédagogiques. Actuellement il est responsable pédagogique de l'option *Maintenance et Sûreté des Systèmes* et responsable des contrats de professionnalisation dans cette même option.

Il effectue la majorité de son service d'enseignement à l'ESSTIN (en moyenne 200h éq. TD/an répartis en C, TD, TP), Il faut ajouter des encadrements de projets et stages (plus de 75 projets de 5ème année, tuteur de 8 étudiants en alternance, plus de 60 stages de fin d'études ingénieur).

CRIStAL - UMR 9189
Cité Scientifique - Bât. M3 extension
59655 Villeneuve d'Ascq Cedex - France
www.cristal.univ-lille.fr

Il intervient aussi depuis 2009 dans le Master Ingénierie des Systèmes Complexes et a effectué plusieurs cours en lien avec ses recherches sur les Réseaux Bayésiens dans d'autres établissements (CENIDET au Mexique, Ecole Centre Paris, ENSEM Univ. Lorraine).

La forte participation à l'encadrement de projets et stages lui permet d'avoir de nombreux contacts industriels qu'il utilise tant pour construire, alimenter ses enseignements que pour développer ses activités de recherche.

Activités de recherche
Monsieur WEBER s'implique dans son laboratoire. Il fait partie du Conseil de Laboratoire CRAN depuis 2006 (membre élu ou nommé), il est membre de la commission Information Scientifique et Technique.

Il a co-encadré 6 thèses de doctorat soutenues en 2007, 2008, 2009, 2011 (2) et 2012. Il co-encadre actuellement une thèse en contrat CIFRE avec EDF. Il a de plus encadré 7 stages de Master.

Les publications sont régulières, de qualité, dans des revues et conférences internationales de bon niveau, principalement spécialisées dans les domaines de la sûreté de fonctionnement et de la maîtrise des risques. Le bilan quantitatif mentionne 20 articles de revues internationales (dont 17 indexées JCR), 1 article de revue nationale, la participation à la rédaction de 6 ouvrages. A noter que 4 articles (dans les revues RESS, EAAI, JRR) sont cités de manière assez importante.

Le bilan de publication dans des conférences est conséquent : 50 articles de conférences internationales et 25 communications dans des conférences nationales. De plus, Philippe WEBER participe régulièrement à des groupes de travail pour y présenter ses travaux ce qui montre sa volonté de communiquer sur sa recherche et promouvoir les outils et méthodes qu'il développe. Cette volonté se traduit aussi par l'organisation de sessions invitées dans des conférences ou par la création et l'animation du GTR *Réseaux probabilistes appliqués à la maîtrise des risques et à la sûreté de fonctionnement* de l'IMdR.

Philippe WEBER collabore avec des collègues de son laboratoire et des chercheurs extérieurs. Il cite en particulier 4 collaborations internationales :

- Université de Concordia, Pr. Youming Zhang, Canada
- Université de Barcelone, Pr. Vincent Puig, Espagne
- Universita del Piemonte Orientale, Pr. Luigi Portinale, Italie
- Queen Mary, University of London, Pr. Martin Neil, Angleterre.

Certaines de ces collaborations ont abouti à des publications co-signées.

Philippe WEBER a participé à 3 projets de recherche européens : FP6 IFATIS 2002-2005, FP7 Dynamite 2005-2009, FP7 F3 Factory 2009-2013 et plusieurs projets de recherches nationaux ou régionaux (ANR, GIS 3SGS, CPER). Il maintient des relations industrielles fortes (parfois en lien avec l'enseignement comme signalé plus haut), en particulier au travers de thèses en contrat CIFRE avec EDF.

Philippe WEBER s'implique dans son établissement d'enseignement (ESSTIN) et dans son laboratoire de recherche (CRAN). Le dossier est bien équilibré entre activités de recherche, pédagogique et administrative. Philippe WEBER développe ses activités en lien fort lien avec le monde industriel : en enseignement par l'intermédiaire des stages, des contrats de professionnalisation, en recherche sous la forme de contrat CIFRE et de participation à des projets.

CRIStAL
Centre de Recherche en Informatique, Signal et Automatique de Lille

Synthèse des travaux de recherche

Les recherches menées par Philippe WEBER se trouvent à l'interface entre d'une part la sûreté de fonctionnement et la maîtrise des risques, et d'autre part la commande et le diagnostic des systèmes dynamiques continus. Ses travaux visent à proposer et utiliser un formalisme de modélisation original et unifié pour garantir un fonctionnement sûr des systèmes commandés. Ceci justifie son appartenance à 2 départements du laboratoire : *Ingénierie des Systèmes Eco-Techniques* (ISET) et *Contrôle, Identification, Diagnostic* (CID), et sa participation à un projet dans chaque département : le projet *Sûreté de Fonctionnement Système* (SdFS - ISET) et le projet *Co-conception de systèmes dynamiques sûrs de fonctionnement* (CSDF-CID).

L'objectif principal des recherches menées par Philippe WEBER est de formaliser des méthodes de construction de modèles probabilistes représentant les bons fonctionnements et les dysfonctionnements d'un système industriel. Ces modèles ont pour but de permettre l'évaluation des objectifs de fonctionnement du système (exigences opérationnelles, performances) et les conséquences en termes de fiabilité et de maîtrise des risques (exigences de sûreté). Ceci nécessite de modéliser les impacts de l'environnement sur le système et sur ses performances, mais aussi l'impact des stratégies de commande et des stratégies de maintenance sur l'état de santé du système.

Le chapitre 3 du mémoire propose une synthèse des différents travaux réalisés. Il est constitué de plusieurs sections logiquement agencées. Les contributions de chacune des thèses co-encadrées sont présentées.
Les principes généraux d'un réseau bayésien et son utilisation pour la sûreté de fonctionnement sont dans un premier temps présentés. Le choix de cette modélisation est motivé, argumenté : un Réseau Bayésien (RB) est un modèle graphique probabiliste qui est bien adapté aux systèmes complexes, multi-composants.
Les modélisations par RB statiques dans le cas booléen, puis dans le cas multi-état, sont présentées successivement. Des exemples simples sont pris pour illustrer les méthodes de construction d'un RB. Ces travaux ont été appliqués sur différents cas d'application (collaboration avec EDF, avec SOREDAB dans le cadre du projet ANR SKOOB) qui sont rapidement présentés. S'agissant d'une synthèse de travaux de recherche, Philippe WEBER n'a pas voulu entrer dans les détails de ces travaux, le lecteur intéressé pourra se référer aux thèses et travaux cités.
Les RB dynamiques sont ensuite présentés. Ces modèles permettent de tenir compte de l'impact de l'environnement et des conditions d'utilisation du système. Là aussi, les explications fournies sont très pédagogiques et les argumentations en faveur de l'utilisation de cette modélisation sont convaincantes.
La dernière section de cette synthèse propose des travaux permettant de faire le lien entre sûreté de fonctionnement et système de commande. Les RBD sont utilisés afin de calculer la pondération (probabilité de contribution d'un actionneur donné lorsque le système fonctionne compte tenu de l'indisponibilité de certains actionneurs défaillants) des commandes du système suractionné. Ceci permet de répartir au mieux les commandes sur un système suractionné (problème d'allocation de commande). La démarche a été appliquée à un réseau de distribution d'eau potable (collaboration avec l'UPC sur le réseau d'eau de la ville de Barcelone). Ces travaux sont originaux et très prometteurs. Ils constituent d'ailleurs un des axes de recherche que Philippe WEBER compte poursuivre et qui est repris dans le chapitre suivant présentant le projet de recherche.
Philippe WEBER conclut ce chapitre en énonçant les différentes contributions de ses travaux et en dégageant les trois apports majeurs :
- modélisation des conséquences fonctionnelles des défaillances
- modélisation dynamique de la fiabilité d'un système multi-composant basée sur la fiabilité des composants dans leur environnement

---

CRIStAL - UMR 9189
Cité Scientifique - Bât. M3 extension
59655 Villeneuve d'Ascq Cedex - France
www.cristal.univ-lille.fr

- synthèse de loi de commande permettant d'optimiser la fiabilité du système.

Les travaux de recherche de Philippe WEBER visent à formaliser et utiliser des modèles probabilistes pour analyser et améliorer la sûreté de fonctionnement d'un système multi-composant. Tout au long de ce chapitre, Philippe WEBER a fait un effort important de synthèse, de clarté, de justification de ses travaux. Cet exposé lui permet de positionner les travaux qu'il a réalisés et d'en montrer la pertinence tant académique que liée à des problématiques industrielles.

Projet de recherche

Le projet de recherche proposé par Philippe WEBER est décrit dans le chapitre 4. Ce projet est dans la continuité de ses travaux antérieurs et concerne donc
- l'intégration de connaissances probabilistes pour optimiser les stratégies de commande des systèmes dynamiques et augmenter la fiabilité des systèmes commandés
- la modélisation probabiliste en maîtrise des risques des systèmes sociotechniques, avec évaluation de conséquences économiques, sociétales et environnementales
- l'extension des modèles graphiques probabilistes à de nouvelles classes de systèmes

Philippe WEBER énonce des perspectives de recherche très pertinentes. Celles-ci sont très bien argumentées et positionnées vis-à-vis des problématiques de recherche intéressant la communauté scientifique et les industriels. Pour développer ce projet, Philippe WEBER souhaite conforter les relations avec des chercheurs de laboratoires français et internationaux. Des pistes de collaborations relativement précises sont décrites.

Conclusions

Le dossier présenté par Monsieur Philippe WEBER témoigne d'un très bon niveau d'activité sur les différentes missions d'un enseignant chercheur. C'est un dossier très bien équilibré entre ces différentes missions. Les activités et orientations pédagogiques et de recherche se nourrissent mutuellement en gardant toujours à l'esprit les problématiques industrielles.
Il a su valoriser ses travaux par des publications internationales de qualité et a acquis une réelle reconnaissance sur son domaine de recherche.
Le chapitre 3 décrivant ses travaux de recherche montre ses compétences pédagogiques, l'originalité de ses recherches dans la communauté scientifique, sa capacité de synthèse et son expertise sur son domaine de recherche. Le chapitre 4 décrit un projet de recherche cohérent, ambitieux et original. Il ne fait nul doute que Philippe WEBER a toutes les capacités pour réaliser et diriger des recherches de qualité.

En conclusion, je donne un avis Très Favorable à la soutenance de Monsieur Philippe WEBER en vue de l'Habilitation à Diriger des Recherches.

Fait à Villeneuve d'Ascq, le 6 Juin 2015.

Vincent Cocquempot
Professeur des Universités
Université Lille1

CRIStAL - UMR 9189
Cité Scientifique - Bât. M3 extension
59655 Villeneuve d'Ascq Cedex - France
www.cristal.univ-lille.fr

LINA – Laboratoire d'Informatique de Nantes Atlantique – UMR CNRS 6241
Équipe DUKe (*Data User Knowledge*) - École Polytechnique de l'Université de Nantes
La Chantrerie - rue Christian Pauc - BP 50609 - 44306 Nantes Cedex 3

Rapport sur le mémoire

« Modélisation graphique probabiliste pour la maîtrise des risques, la fiabilité et la synthèse de lois de commande des systèmes complexes »

présenté par M. Philippe WEBER
en vue de l'obtention de l'habilitation à diriger les recherches de l'Université de Lorraine

---

Les travaux de recherche de M. Philippe WEBER, effectués ces vingt dernières années, se situent dans le domaine de la maîtrise des risques et de la fiabilité et apportent des contributions dans l'utilisation de modèles graphiques probabilistes pour la résolution de plusieurs problèmes liés à la sûreté de fonctionnement : modélisation en maîtrise des risques, en maintenance et en fiabilité pour des systèmes socio-techniques complexes, et intégration de connaissances de fiabilité dans la commande et le diagnostic de systèmes automatisés.

La partie scientifique du mémoire est structurée en deux grandes parties avec une introduction motivant les travaux du candidat, et la présentation de ses activités de recherche, puis le descriptif d'un projet de recherche en trois axes.

La première partie « Présentation des activités de recherche » décrit brièvement la problématique générale abordée par M. Weber et présente les différences contributions du candidat en liaison avec les collaborations industrielles et/ou encadrements de thèses. sur lesquelles étaient adossées ces travaux.
M. Weber propose une démarche scientifique de formalisation de méthodes de construction de modèle exploitant la flexibilité et l'efficacité de la représentation par modèles graphiques probabilistes. Il nous décrit ainsi l'utilisation de modèles de plus en plus complexes (réseaux bayésiens « statiques », puis dynamiques, puis modèles relationnels probabilistes) dans différents contextes.
M. Weber nous décrit progressivement, et de manière très pédagogique ses travaux concernant l'utilisation de Réseaux bayésiens comme formalisme de modélisation pour la sûreté de fonctionnement, puis pour la modélisation de la fonction de structure des systèmes complexes et multi-états. Il décrit ensuite ses contributions concernant l'utilisation de réseaux bayésiens dynamiques pour représenter la fiabilité des composants d'un système intégrant l'impact de l'environnement et des conditions d'exploitation, puis pour l'intégration de la fiabilité à la commande des systèmes continus.
L'hypothèse générale faite par M. Weber est que les données nécessaires pour l'utilisation de méthodes d'apprentissage automatique ne sont pas suffisantes, et qu'il faut construire ces modèles par expertise et analyse de formalismes métiers (AMDEC, HAZOP, SADT, …). Les travaux proposés ici montrent très bien comment ces connaissances métiers guident la construction de la structure graphique du modèle. Il aurait été intéressant de compléter cela par une présentation plus détaillée de la détermination des paramètres (tables de probabilité conditionnelles) à partir de ces mêmes connaissances métiers ou d'expertise.
L'hypothèse initiale, réaliste, mériterait aussi d'être nuancée, en prolongeant les travaux actuels pour essayer de conjuguer à la fois données et connaissances métier, en faisant le lien avec d'autres travaux du domaine utilisant des données de retour d'expérience.

Les travaux présentés ici se situent à l'intersection entre sûreté de fonctionnement et modèles probabilistes. Philippe Weber est l'une des personnes pouvant s'afficher comme spécialistes à la frontière de ces deux domaines, mais ce n'est pas le cas de tous les lecteurs potentiels de ce manuscrit. Il aurait donc pu être intéressant de compléter le document avec une présentation plus détaillée des extensions des modèles graphiques mis en œuvre (pour le lecteur plutôt expert en sûreté de fonctionnement) ou des outils de sûreté de fonctionnement évoqués (pour le lecteur expert en modèles graphiques probabilistes).

Dans la deuxième partie, « Projet de recherche », M. Weber décrit ses perspectives de manière cohérente, sous des angles à la fois méthodologique et applicatif, avec trois grands axes.
Le premier axe correspond à l'intégration de connaissances probabilistes dans la stratégie de commande des systèmes dynamiques, avec la mise en œuvre de réseaux bayésiens dynamiques complexes intégrés dans des algorithmes de commande.
Le deuxième axe concerne la modélisation probabiliste en maîtrise des risques des systèmes socio-techniques et leur impact sur le développement durable. Pour cela, M. Weber souhaite étendre les modèles relationnels probabilistes à un autre formalisme de représentation de l'incertain, les fonctions de croyance, comme cela avait été le cas pour les réseaux bayésiens classiques.
Le dernier axe se propose de travailler sur la formalisation des modèles graphiques probabilistes en sûreté de fonctionnement pour de nouvelles classes de systèmes.
L'utilisation et/ou l'adaptation de modèles graphiques probabilistes complexes comme les modèles dynamiques ou relationnels me semble particulièrement pertinent, et je vois clairement où se situent les challenges en terme de modélisation soulevés par M. Weber. Par contre, en tant que non spécialiste dans le domaine de la maîtrise des risques et de la fiabilité, je pense que le projet de recherche proposé aurait gagné à être situé plus clairement par rapport aux grands défis « ouverts » dans ce domaine qui est le cœur de métier de M. Weber.
M. Weber complète cette partie de son manuscrit en décrivant l'insertion des différents axes de ce projet de recherche dans un cadre collaboratif, aussi bien académique qu'industriel, en démontrant une volonté de collaborations au niveau national mais aussi internationale.

La partie scientifique de ce mémoire est précédée de deux chapitres résumant le curriculum vitae de M. Weber et ses activités d'enseignement et d'administration, non négligeables. Les activités d'enseignement de M. Weber, et de responsable de la formation en maintenance et en sûreté de fonctionnement à l'ESSTIN, le mettent au cœur du triptyque Recherche-Formation-Innovation en lui permettant à la fois de former des ingénieurs par la recherche et de travailler en étroite collaboration avec des industriels du domaine autant pour l'enseignement que la recherche.

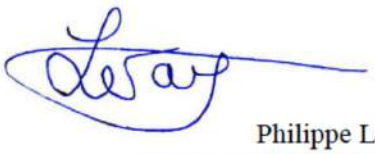
Les activités de recherche de M. Weber sont très satisfaisantes et adossées à des projets contractuels aussi bien nationaux qu'internationaux. Ses collaborations scientifiques nationales et internationales avec d'autres chercheurs de haut niveau sont nombreuses et bien mises en avant dans la partie scientifique du manuscrit. Il a co-encadré 6 thèses soutenues entre 2007 et 2012 et co-encadre une autre thèse dont la soutenance est prévue en 2016. M. Weber a aussi une forte activité d'encadrement de stages. Il co-organise régulièrement des sessions invitées dans les conférences nationales ou internationales du domaine. De plus, il est co-fondateur et animateur d'un groupe de travail et de réflexion au sein de l'Institut pour la Maîtrise des Risques.

Ses travaux de recherche sont significatifs tant du point de vue théorique que du point de vue applicatif. Les résultats des travaux de M. Weber ont donné lieu à 21 publications en revue (dont 17 internationales indexées par JCR) et ont fait l'objet de présentations dans de très nombreuses conférences de haut niveau, autant au niveau international que national. M. Weber est aussi co-auteur de 6 chapitres de livres.

En conclusion, M. Weber s'est attaché à développer des travaux de recherche pertinents et reconnus internationalement concernant l'utilisation de modèles graphiques probabilistes en sûreté de fonctionnement. Ses contributions et son projet de recherche montrent que M. Weber fait preuve d'une stratégie autonome de recherche scientifique. Le descriptif de ses activités scientifiques illustrent aussi sa capacité à encadrer de jeunes chercheurs.

Pour toutes ces raisons, je donne un avis très favorable à la présentation des travaux de M. Philippe Weber, en vue de l'obtention du diplôme d'habilitation à diriger les recherches de l'Université de Lorraine.

Rédigé à Nantes, le 20 mai 2015



Philippe LERAY
Professeur des Universités
Équipe DUKe (*Data User Knowledge*)
Laboratoire d'Informatique de Nantes Atlantique (LINA)

Cinq Publications Majeures

Medina-Oliva G., Weber P., Iung B. PRM-based patterns for knowledge formalisation of industrial systems to support Maintenance Strategies Assessment. *Reliability Engineering and System Safety*, 116, August (2013), pp. 38-56.

Weber P., Medina-Oliva G., Simon C., Iung B. Overview on Bayesian networks Applications for Dependability, Risk Analysis and Maintenance areas. *Engineering Applications of Artificial Intelligence*, 25(4), June (2012b), pp. 671-682, DOI:10.1016/j.engappai.2010.06.002

Guenab F., Weber P., Theilliol D., Zhang Y.M. Optimal Design of Fault Tolerant Control System versus Reliability Analysis under Dynamic Behaviour Constraints. *International Journal of Systems Science*, 42(1), (2011), pp. 219-233.

Khelassi A., Theilliol D., Weber P. Reconfigurability Analysis for Reliable Fault-Tolerant Control Design, *International Journal of Applied Mathematics and Computer Science* (AMCS), 21(3), (2011), pp. 431-439.

Weber P., Jouffe L. Complex system reliability modelling with Dynamic Object Oriented Bayesian Networks (DOOBN). Special Section - Selected Papers Presented at QUALITA 2003, guest editors J.F. Aubry *in Reliability Engineering and System Safety*, 91(2), (2006), pp. 149-162.

Reliability Engineering and System Safety 116 (2013) 38–56

Contents lists available at SciVerse ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

PRM-based patterns for knowledge formalisation of industrial systems to support maintenance strategies assessment

G. Medina-Oliva *, P. Weber, B. Iung

CRAN—Université de Lorraine, CNRS UMR7039, Campus Sciences, BP 70239, 54506 Vandoeuvre, France

ARTICLE INFO

Article history:
Received 18 October 2012
Received in revised form
25 February 2013
Accepted 26 February 2013
Available online 21 March 2013

Keywords:
Maintenance strategies
Performances analysis
Decision-making
Bayesian Networks (BN)
Probabilistic Relational Model (PRM)

ABSTRACT

The production system and its maintenance system must be now developed on "system thinking" paradigm in order to guarantee that Key Performance Indicators (KPI) will be optimized all along the production system (operation) life. In a recursive way, maintenance system engineering has to integrate also KPI considerations with regards to its own enabling systems. Thus this paper develops a system-based methodology wherein a set of KPIs is computed in order to verify if the objectives of the production and maintenance systems are satisfied. In order to help the decision-making process for maintenance managers, a "unified" generic model have been developed. This model integrates (a) the interactions of the maintenance system with its enabling systems, (b) the impact of the maintenance strategies through the computation of some key performance indicators, and (c) different kinds of knowledge regarding the maintenance system and the system of interest, including quantitative and qualitative knowledge. This methodology is based on an executable unified model built with Probabilistic Relational Model (PRM). PRM allows a modular representation and inferences computation of large size models. The methodology added-value is shown on a test-bench.

1. Introduction

Nowadays high competitiveness makes industrial enterprises search higher performances such as higher quality products, lower costs, sustainability, etc. [32]. To achieve these requirements, the main relevant challenge is to optimize the operations of the production system (operational level), called here after System of Interest (SoI) [26] within its whole life-cycle and in consistence with tactical and strategic considerations (i.e. MES[1] and ERP[2] layers). More precisely, it implies that the SoI has to be controlled as "optimal" during all the Maintaining in Operational Condition (MOC) phase (to sustain the system in operational conditions). Indeed, for example, [2] highlights that usually the MOC cost is much higher than the acquisition and operation costs. This fact leads to the consideration of the optimization not only the SoI by itself but also of all its enabling systems as well as the interactions developed between them. In that way, one important enabling system to be taken into account is the Maintenance System (MS) since its role has changed dramatically in regards to its obvious impact on improving availability, performance efficiency, products quality, on-time deliveries, environment-safety requirements, and total plant cost effectiveness at high levels [2]. Thus in order to control/improve business-operational considerations, maintenance managers should take decisions about the maintenance strategies to be implemented as well as the necessary resources to satisfy SoI performances and requirements [65]. These decisions result from models allowing maintenance performances quantification. According to [73], the items to be formalized most of the time within these models are: the parameter triggering maintenance actions, the performance criteria to be optimized, the restoration degree of the components after a maintenance action and the architecture of the system (i.e. single-component or multi-components). Nevertheless, this formalization does not support the knowledge treating the characteristics of the SoI and of the MS within a "system thinking" to support better optimization from their mutual interactions [73]. In addition, formalization does not consider, in a recursive way, the interaction of the MS with all its

Abbreviations: KPI, Key Performance Indicators; PRM, Probabilistic Relational Model; BN, Bayesian Networks; OOBN, Object Oriented Bayesian Networks; SoI, System of Interest; MS, Maintenance System; MOC, Maintaining in Operational Condition; SKOOB, Structuring Knowledge with Object Oriented Bayesian nets; COTS, Components Off The Shelf principle; HD, Having to Do flow; AD, Able to Do flow; WD, Wanting to Do flow; KHD, Knowing How to Do flow; FT, Fault Trees; POF, Pathogenic Organizational Factors; SADT, Structured Analysis and Design Technique; FMEA, Failure Mode and Effects Analysis; HAZOP, HAzard and OPerability Study; OF,, Output Flow; SP, Support State; IF, Input Flow; AGAN, As Good As New; ABAO, As Bad As Old; MUT, Mean Up Time; MDT, Mean Down Time; DAG, Directed Acyclic Graph; CPT, Conditional Probability Table

* Corresponding author. Tel.: +33 3 83684438.
E-mail addresses: gabriela.medina-oliva@uni-lorraine.fr (G. Medina-Oliva), philippe.weber@uni-lorraine.fr (P. Weber), benoit.iung@uni-lorraine.fr (B. Iung).

[1] Manufacturing Execution System.
[2] Enterprise Resource Planning.

0951-8320/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ress.2013.02.026

enabling systems (i.e. its human and organizational systems, its logistic system and nowadays environmental factors) which are necessary to quantify failure scenarios and risky situations.

In that sense, the main characteristics of the SoI to be formalized for supporting maintenance strategies assessment in a "system thinking vision" (with MS) should be:

- Dependences between events such as failures [66].
- Multi-criteria performances [53].
- Different points of views on the SoI but also on the MS: functional, dysfunctional, financial, informational and organizational ones.
- Interactions between the MS and the SoI and its other enabling systems [26].
- Integration of qualitative information with quantitative knowledge on different abstraction levels [13,52].

To be in phase with this system vision for SoI–MS formalization, an original methodology is proposed in this paper wherein a set of Key Performances Indicators (KPI) is computed and used to assess whether the functional architecture of the maintenance system and its associated strategies satisfy the objectives of the SoI and its enabling requirements. If the objectives are not achieved, one must identify the causes which impact on the requirements deviations to support optimization. The assessment is done by simulations on a unified model built from the main characteristics of the SoI and of the MS.

In relation to this proposal, Section 2 presents the problem statement about assessing maintenance strategies for representing industrial reality. Section 3 is underlining the maintenance strategies assessment with regards to SoI considerations. Then Section 4 is describing the methodology to obtain a Probabilistic Relational Model (PRM)-based unified model. The methodology is applied in Section 5 in the case of a real harvest production system to show its feasibility and interest for maintenance/production optimization. Finally, conclusions and prospects are given in Section 6.

2. Problem statement on maintenance strategies assessment with regards to SoI considerations and proposed methodology

2.1. Maintenance strategies assessment

There are several works in maintenance strategies assessment but few treat the characteristics of both the SoI and the MS within a "system thinking" to support better optimization from their mutual interactions [73].

Indeed generally, maintenance strategies characterization should be based on the following criteria:

- System dimension (mono or multi-components) [35].
- Degradation/failure modeling (malfunctioning of the SoI) [12,24,71].
- Multi-performances and multi-levels system [53].
- Maintenance actions (to be defined for MS) based on the standard [15].
- MS interactions with its own enabling systems but also with its environment [26,31,68].
- Tools required for multi-components system modeling [14,22,46].

Nevertheless, some models developed for assessing maintenance strategies such as proposed by [12] consider just single-component systems, or [70] assess only the availability, cost or reliability as KPI. These models are far away from the industrial reality and different lacks can be identified for most of the existing models:

- Integration of multi-criteria performances: models focus on the assessment of availability, reliability and costs criteria. They do not integrate the MS impact on other performances such as quality, risk, etc. [53].
- Integration of the impact of organizational and human aspects within system performances [39,68], while focusing only on the technical items of systems (e.g. degradation mechanisms, maintenance actions frequency, etc.).
- Consideration of multi-component systems. This consideration leads to dependences between components such as stochastic, structural and economical ones. However, current models treat mainly only single-component systems. These models make implausible and unrealistic assumptions far away from industrial systems (composed of a lot of components) [11,35].
- Development of modular and generic models which consider the interactions between the MS and SoI. This is a limit for model reuse [63][3] and does not allow to address the issue related to big-size models.

Thus, relevant issues have to be considered to develop more realistic models for production/maintenance optimization such as integration of multi-criteria performances (i.e. non conventional KPI have to be calculated), integration of the impact of organizational and human systems both on MS and SoI operations (i.e. consideration of heterogeneous knowledge issued from different areas), consideration of multi-component systems, design of modular and generic models that support knowledge capitalization such as proposed by Components Off The Shelf (COTS) principle, and definition of assembling—aggregation mechanisms to be applied to COTS for supporting the different abstraction layers of systems.

To face these previous issues, the proposed contribution developed in this paper consists mainly in defining an original methodology to model both the characteristics of the SoI and of the MS in order to assess, by computing a set of indicators, if the MS functional architecture and its maintenance strategies (defined by means of the maintenance plan and its organization), are able to optimize the SoI KPIs and the enabling system requirements. In that way, an "unified" model based on generic patterns was developed for the maintenance managers integrating: (a) SoI characteristics, (b) MS characteristics, (c) the interactions of the MS with its enabling systems, (d) interactions between SoI and MS, (e) the impact of the several maintenance strategies through the computation of some KPI and (f) knowledge of diverse natures such as qualitative (organizational and human analyses) and quantitative (technical analyses) one.

The unified model is developed with an extension of Bayesian Networks (BN) which is a technique well justified by [7,36,37,43] with the purpose of estimating–improving performances such as the reliability and the availability. This modeling method is not the solution to support all the issues previously mentioned but it seems to fit in the context of complex systems modeling [76]. Thus, our proposal consists mainly in formalizing a methodology to define patterns based on an extension of Object Oriented Bayesian Networks called the Probabilistic Relational Model (PRM) [19,20,33]. These PRM-patterns could be later assembled for modeling all the aspects of industrial system knowledge in order to help decision-making for maintenance and dependability domains.

This research has been conducted in the frame of the SKOOB project[4] sponsored by the French National Research Agency. This

[3] Structuring Knowledge with Object Oriented Bayesian nets.

[4] http://skoob.lip6.fr/doku.php?id=public:texte_anglais_de_presentation.

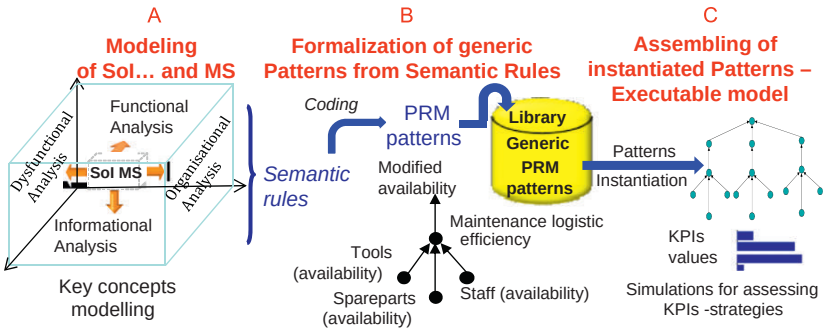


Fig. 1. Methodology to build a PRM model for assessing maintenance strategies.

project focused, from industrial needs, on the development of a generic model based on PRM which enables to solve complex models in risk analysis, maintenance and dependability, applied to various socio-economic systems of strategic importance (nuclear, food industries, medical or social organizations) [17,21,63].

2.2. Methodology for SoI–MS knowledge formalization

The unified model has to result of a methodology generic enough and not totally dependent (a) on the modeling technique selected and (b) on the ability of the engineer implementing it. In that way, it was decided, firstly to define semantic rules in a description language materializing the main concepts of the MS and of the SoI as well as the relationships between these concepts. Secondly to formalize the semantic rules in a quantitative tool, represented as PRM-based generic patterns. Finally to instantiate patterns and assemble them in the case of a specific application. Therefore the proposed methodology is based on the following steps:

- Identification of key knowledge concepts (i.e. function, flows) related to SoI modeling (Fig. 1A). Knowledge formalization starts from a functional analysis and considers the abnormal operation [29,78]. Then the informational point of view and the organizational one are developed. The relationships between these concepts are formalized by the definition of semantic rules specific to SoI.
- Use of the same key knowledge concepts for identifying the semantic rules related to MS. This identification is done by developing similar analyses for the MS as those performed for the SoI modeling. In addition, semantic rules also link the concepts of the SoI with MS concepts allowing to identify the impact of the MS on the SoI performances (Fig. 1A).
- Formalization of PRM patterns based on semantic rules. Patterns are represented in a graphical way as BN (Fig. 1B).
- Instantiation of the generic patterns for a particular case study. Instantiated patterns are then assembled with regards to a same abstraction level or different abstraction levels. A global and executable model can be created for performing simulations to assess maintenance strategies and their impacts on SoI (Fig. 1C).

3. Definition of semantic rules from concepts issued of multi-points of views modeling on the SoI and on the MS modeling (Fig. 1A)

3.1. Knowledge formalization of the SoI

3.1.1. SoI knowledge modeling

In consistence with the "systemic paradigm" advocated in "System Theory in General" [72], the main concepts used for structuring the SoI knowledge are the concepts of Functions, Components and Flows (produced or consumed by function) knowing that Flows can be classified with different Modalities.

- A function is an action performed by a "mechanism" (component, person, etc.) that transforms an input flow into an output flow. A global function (at the highest abstraction level) can materialize the finality of the system (global mechanism). Thus, a function can be decomposed into sub-functions (to represent sub-systems levels) until elementary functions which are performed (supported) by components (i.e. pump, valves, and engine). At a same abstraction level, the relations between functions are represented by the flows they exchanged (the output flow of a function can become the input flow of the downstream function).
- A flow can be modality-typed as proposed by Mayer et al. [45] with "Having to Do flow" (HD), "Able to Do flow" (AD), "Wanting to Do flow" (WD), "Knowing How to Do flow" (KHD). These four types of flows could be instantiated as Inputs of the function but also as Outputs of the function. A Flow is composed of a lot of Objects (i.e. A Flow of Parts is composed of a lot of Parts).

For the SoI knowledge formalization, these general concepts have emerged, firstly from a SADT[5]-based functional analysis allowing identifying the functions and sub-functions realized by the SoI, the flows produced and/or consumed by each function and the components which are supporting the elementary functions [40]. Then, the degraded and failure states of the components but also the flows deviations and their impacts on the output flow of the SoI, are detailed on FMEA[6] and HAZOP[7] analyses. A class diagram representation allows the definition of the flow attributes or properties. The organizational analysis and the Pathogenic Organizational Factors (POF) [38], such as production pressure impacting operators' performance, are modeled within organizational analyses. Finally the qualitative causal relations, between functions through flows exchanges in which the output flow of a function becomes the input flow of the downstream function, are specified [47].

3.1.2. SoI semantic rules

Semantic rules can be described to materialize the relationships such as cause-effects relationships between the different knowledge concepts. They are based on the first logic order. This formalism allows the representation of generic and qualitative relationships independent of the modeler capabilities. It supports the semantic rules reusing since the common concepts (i.e. generic

[5] Structured Analysis and Design Technique.
[6] Failure Mode and Effects Analysis.
[7] HAzard and OPerability Study.

Table 1
SoI semantic rules.

Logic propagation relationship (semantic rules) and output flow (OF)
IF_Nominal ∧ SP_Nominal → OF Nominal
IF_Deviated ∧ SP_Nominal → OF_Deviated
IF_Nominal ∧ SP_Degraded → OF Deviated

concepts) of a system are represented. Moreover, semantic rules could be used to build any quantitative formalism such as Petri Nets, Fault Trees, etc. (e.g. for simulation purposes).

For example, some semantic rules of the SoI define the influence of some input flows and of the support of a function into the output flow of the function [29]. These rules link both the deviations of input flow and the degradation of the support of the function, to the performances of the output flow of the function as proposed by Léger et al. [40] in the form of the following logic equation:

$$\textit{State of the input flow} \wedge \textit{State of the component} \rightarrow \textit{State of the output flow} \quad (1)$$

This generic relationship has been used for the formalization of all the SoI concepts (Table 1) in consistence with works previously done by [40,50].

To synthesize, the main items within the semantic rules of the SoI are:

- The "output flow HD" is considered in a nominal state if all the input flows of the function as well as the support component are in nominal state.
- The "output flow HD" complies function's requirements when its attributes (morphologic, spatial or temporal requirements) are in a nominal state.
- One deviation of the "output flow HD" of a function will produce deviations on the "input flows HD" of the downstream functions (propagation principle of deviation/failure through flow exchanges between functions).

The same concepts can be translated to formalize MS knowledge.

3.2. Knowledge formalization of the MS

3.2.1. MS knowledge modeling

3.2.1.1. Functional point of view of the MS. The main function performs by the MS is "to maintain the components of the SoI". This function transforms the state of a component (degraded, failed) into an improved state (fixed, nominal). The generic modalities of flows can be thus instantiated as follows for the MS function (Fig. 2):

Main input flows:

- The "component to be maintained" represents the Having-to-Do (HD) flow, so it is the main flow transformed by the function.
- The tools, spare parts, maintenance operators, etc. needed to perform maintenance actions are representing the Able-to-Do (AD) flow.
- The Wanting-to-Do (WD) is an informational flow that triggers the maintenance actions. Maintenance actions are triggered with degradation or deviation indicators, calendar or operational time within the CMMS,[8] the failure of a component, etc. according to the maintenance strategy implemented.
- The Know-How-to-Do (KHD) flow is defined by the importance of procedures to perform a maintenance action correctly (e.g. the organizational point of view).

Main output flows:

- The HD flow is the "maintained component".
- The AD flow is, for example, materials to be recycled.

So, from the formalization made previously, dependences (basis for the semantic rule formalization) of the key elements of the MS function (such as tools, staff, etc.) on the output flow named "maintained component" were defined.

3.2.1.2. Informational point of view of the MS. Now, the flows attributes of the function "to maintain the components of the SoI" are formalized in a class diagram. This diagram shows the relationships between different objects (of the flows) as well as the attributes of these objects. It highlights some elements that are not represented in the functional point of view such as the interactions of the component with the environment, the specialization of maintenance actions or the attributes of each action such as the costs associated, the duration and their restoration degree. This diagram is an extension of the class diagrams proposed in [48] and in the standard [25]. Fig. 3 illustrates the relationships between different objects related to the MS function and the interaction of the MS with the SoI within a UML-based class diagram.

From the class diagram, relevant items must be underlined in relation to MS considerations:

- A maintenance plan is composed of a set of maintenance actions required for maintaining in operational conditions the component. Therefore: Maintenance plan={maintenance actions}. A maintenance action is characterized mainly with two attributes: its duration and its restoration degree.
- Traditionally two types of maintenance strategies are distinguished: corrective and preventive. Within preventive strategy, it is possible to define three categories such as time-based, condition-based and predictive maintenance [15].
- One of the main attributes of maintenance action is its impact on the component's state (health condition). In consistence with [23,57], three ways can be detailed to characterize the restoration degree of an action (intervention): perfect (AGAN—As Good As New), minimal (ABAO—As Bad As Old) and imperfect [4,42].
- Condition-based and predictive maintenance are structured on the monitoring of the representative variables of degradation such as symptoms or flow deviations. One of the main characteristics of this kind of maintenance is the reliability of its monitoring system [74]. In fact, the monitoring process is delivering sometime some errors such as false alarms or non-detections [3,10,18]. It is important to take into account this aspect because the reliability of a monitoring system impacts the types of maintenance actions. Indeed a non-detection of a degradation level on a component could cause a failure generating over-costs due to a corrective action instead of a preventive one. On the other side, if a false alarm takes place, a preventive intervention may be performed on a good-state-component. In this case the preventive action will be considered as minimal, since it does not improve the state of the component and its availability is decreased due to the down time produced by the intervention. There is also an over-cost.
- The duration of maintenance action depends on maintenance logistic that is implemented (operators' performance, training, stock of spare parts, tools, documents, etc.) besides of course of

[8] CMMS: Computerized Maintenance Management System.

Table 2
Causalities relationships between the mean up time and the variables associated to the implementation of maintenance strategies.

Initial conditions	Input flow (IF) (or attribute of the input flow) Effectiveness of the staff	External conditions Environment	Logic propagation relationship (semantic rules) and output flow (OF)
$MUT_{PLANNED}$	Effective staff	Nominal environment	Effective Staff ∧ Nominal environment → $=MUT_{PLANNED}$
	Ineffective staff	Nominal environment	Ineffective Staff ∧ Nominal environment → $<MUT_{PLANNED}$
	Effective staff	Non-nominal environment	Effective Staff ∧ Non-nominal environment → $<MUT_{PLANNED}$
	Ineffective staff	Non-nominal environment	Ineffective Staff ∧ Non-nominal environment → «$MUT_{PLANNED}$

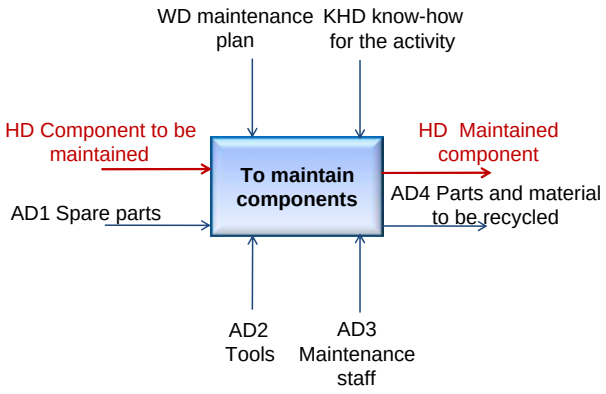


Fig. 2. MS main function.

the "ability" of a component to be maintained or restored (easiness to diagnostic, component accessibility etc.) (CEI 60300-3-14).
- The external conditions, in which a component is operating, are exogenous variables of the MS. However they impact the performances of a system, more specifically the evolution of its degradation mechanisms and so the mean up time (MUT) and the availability of the component.

These flows attributes and their relationships are considered for the formalization of MS semantic rules.

3.2.1.3. Dysfunctional point of view of the MS. The malfunctioning point of view is a complementary view with the functional one. It aims at analyzing the states of malfunctioning of a component as well as the deviations on the input and output flows of the function. These deviations are represented in the HAZOP studies and FMEA studies. For the MS, an example of deviation could be the availability or unavailability (deviation: NOT OF availability) (e.g. NOT is an HAZOP Deviation Guide Word) of a human/logistic factors.

3.2.1.4. Organizational point of view of the MS. Maintenance operators (e.g. maintenance staff) are influenced by an organizational context. The organizational point of view studies different pathogenic organizational factors (POF) that influence the efficiency of maintenance operators' actions. For example, a component may be replaced but may not be in a perfect state since it was not well-installed by operators due to lack of skills. This fact underlines the lack of a training program to improve operators' skills, which reflects a negative influence of management decisions (organizational context) [39]. Thus, the components' performances depend not only on the impact of maintenance actions but also on the socio-technical environment they are surrounded [60]. In that sense, human actions are impacted by the organizational context generated by the management of an enterprise. This point of view integrates the "KHD flow" of the MS main function. It deals with the knowledge and experience of humans and how it could impact on SoI performances.

A short list of some commons factors found in the domains of nuclear, oil and aviation industries [39,51,60] is defined as follow: failure in daily safety management, weakness of control bodies, poor handling of organizational complexity, no re-examining of the design hypotheses, shortcomings in the organization culture of safety, difficulty in implementing feedback experience and production pressures.

3.2.2. MS semantic rules

MS modeling allows to formalize causality relationships between the decisional variables (main concepts) and their impact on component performances. One of parameters on a component is its "mean up time" (*MUT*). Its dependences are shown as follow:

$$MUT = f(\textit{nature of maint enance actions}\ (\textit{strategy and restoration degree}),\ \textit{human effectiveness}, \textit{environment}\ldots)$$

A *MUT* of reference is established from this general expression. This *MUT* is issued once maintenance actions of diverse natures are performed. The result is a mean up time "planned" which it called $MUT_{PLANNED}$. Table 2 shows how $MUT_{PLANNED}$ is affected by other factors such as the environmental and human factors (semantic rules). Once the component is subjected to «non-nominal» conditions, it will degrade faster and the functioning time will decrease. In addition, if the staff is not qualified to perform maintenance tasks, it is very likely that the component will be repaired in a wrong way which implies a *MUT* decreased.

It is also possible to assess the impact of decisional variables in other components' parameters such as the mean down time (*MDT*). This parameter depends on the failure nature, the maintainability of the component and it is modified also by other factors such as expressed below:

$$MDT = f(\textit{Availability of material and staff resources}\ (\log \textit{istics}), \textit{staff effectiveness},\ldots)$$

In relation to a $MDT_{PLANNED}$, the causality relationships (semantic rules) are defined in Table 3. For example, if one of the input flows of the function "to maintain the component" is deviated, then the $MDT_{PLANNED}$ increases. This deviation is bigger when several input flows are deviated.

In a similar way, the causality relationships are formalized about the decisional variables within maintenance strategies assessment (input flows or an input flows' attributes) and their impact on the SoI performances such as costs and produced quality (Table 4).

These rules highlights that the deviation of an input flow attribute of the MS function, impacts SoI and MS performances. For example in the case of the time-based maintenance, a preventive intervention periodicity too short results on an availability decreasing and a cost increasing. Moreover, a longer periodicity results into important

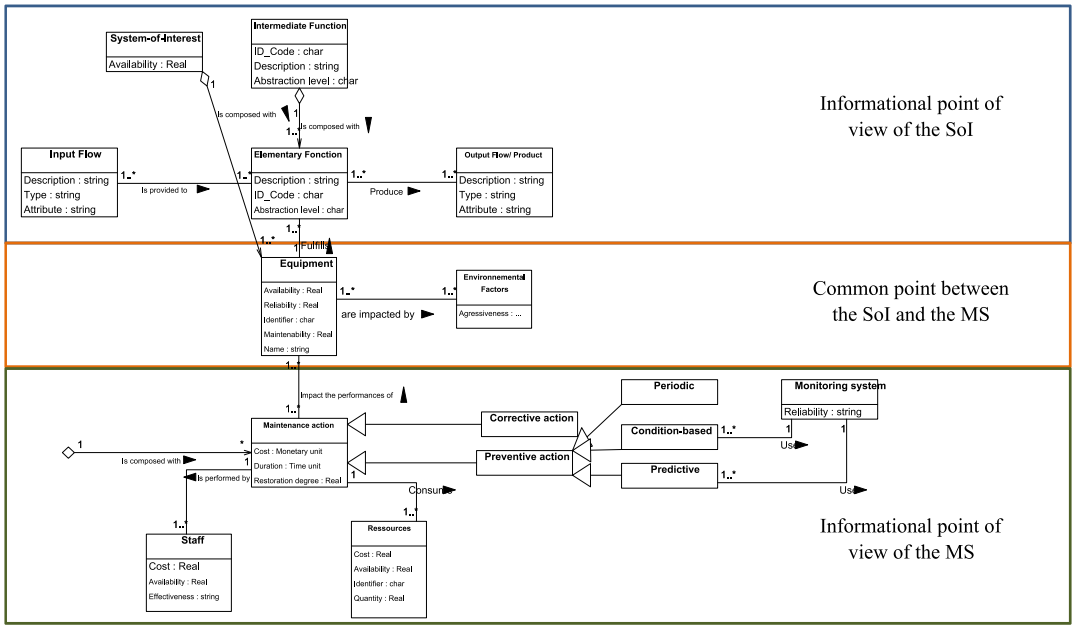


Fig. 3. Attributes and relationships between objects of the MS and SoI.

Table 3
Causalities relationships between the mean down time and the variables associated to the implementation of maintenance strategies.

Initial conditions	Input flow (IF) (or attribute of the input flow)				Logic propagation relationship (semantic rules) and output flow (OF)
	IF1-AD availability tools	**IF2-AD availability spare parts**	**IF3-AD availability staff**	**IF4-AD effectiveness of the staff**	
$MDT_{PLANNED}$	IF1-AD available tools	IF2-AD available spare parts	IF3-AD available staff	IF4-AD effective staff	IF1-AD available tools ∧ IF2-AD available spare parts ∧ IF3-AD available staff ∧ IF4-AD effective staff → $=MDT_{PLANNED}$
	IF1-AD unavailable tools	IF2-AD unavailable spare parts	IF3-AD unavailable staff	IF4-AD ineffective staff	IF1-AD unavailable tools ∧ IF2-AD unavailable spare parts ∧ IF3-AD unavailable staff ∧ IF4-AD ineffective staff → »$MDT_{PLANNED}$

Table 4
Causalities relationships between maintenance input flows and maintenance performances.

Logic propagation relationship (semantic rules)
(1) *IF1-AD Inadequate Maintenance Plan* ∧ *IF2-AD Unavailable resources* ∧ *IF3-AD Unavailable resources* ∧ *Non-Nominal environment* → < $Availability\_{PLANNED}$
(2) *IF1-AD Inadequate Maintenance Plan* ∧ *IF2-AD Unavailable resources* ∧ *IF3-AD Unavailable resources* ∧ *Non-Nominal environment* → > *Maintenance Costs*
(3) *IF1-AD Inadequate Maintenance Plan* ∧ *IF2-AD Unavailable resources* ∧ *IF3-AD Unavailable resources* ∧ *Non-Nominal environment* → < *Expected Quality*

failure risks; a more degraded component and thus other performances could be impacted such as the produced quality. The availability of resources (i.e. tools, spare parts, etc.) also impacts the availability of the system as well as the costs of the SoI & MS. The analysis of these factors and their interactions are needed to quantify performances in order to help decision-making.

To synthesize the content of this section, the following semantic rules are proposed:

The deviation of one "input flow" of the MS function produces a deviation on the attribute "availability" of the output flow "HD maintained component".

Therefore

- The deviation "less availability" of the input flows AD "tools, spare parts, staff, etc." increases the attribute "duration of the maintenance action" producing a decrease of the attribute "availability" of the output flow "HD maintained component" (deviation of the expected value of the availability).
- The deviation "ineffectiveness" of the input flow "AD staff" decreases the attribute "availability" of the output flow "HD maintained component" (deviation of the expected value of the availability).

- A "non-nominal" (aggressive) environment (deviation compared to nominal conditions) decreases the attribute "availability" of the output flow "HD maintained component" (deviation of the expected value of the availability).
- The deviation of the parameters of the input flow "WD Maintenance plan" (i.e. periodicity of time-based actions) decreases the attribute "availability" of the output flow "HD maintained component" as well as other performances of the MS and of the SoI (deviation of the expected value).
- The "reliability of the monitoring system" is modifying a part of the condition-based/prediction actions within the predefined maintenance plan. In that sense, the deviation "NOT" of the attribute "detection" probably generates a failure (corrective action). The deviation "MORE" of the attribute "detection" (i.e. false alarms) generates a preventive action of a good state component.

These semantic rules allow the formalization of the basic concepts of MS and of the SoI. However, to assess the impact of maintenance strategies choices on SoI and MS performances, knowledge of both systems should be linked. In that way, the concept that links the two systems is the "component" concept. The component is maintained by the MS and then it is used as an input flow to support the function of the SoI.

Since semantic rules are expressed in a "logical language" purely qualitative, they are not sufficient to support maintenance strategies and KPI assessments because quantitative simulation is needed. For example, it is necessary to quantify the availability of components/system based on the probability to have input flows available. In that way, it is required to use these rules to build executable and generic patterns in order to create a model that allows the assessment of KPI with regards to different maintenance strategies.

4. Knowledge unification and integration within PRM

4.1. Pattern definition

"A pattern describes a problem which occurs over and over again in our environment, and then describes the core of the solution to that problem, in such a way that you can use this solution a million times over, without ever doing it the same way twice" [1]. In the context of this work, the "problem" is related to maintenance strategies assessment. Thus in order to capitalize knowledge and model-reuse, it is possible to build patterns allowing a modular representation of the representatives variables both of the SoI and MS. These variables are given by the semantic rules and can lead to create "patterns" which can be associated linking variables defined in the rules (Fig. 1A). Indeed, the different aspects of the MS and of the SoI should be integrated thanks to the characteristics of the systems described in the rules. This integration enables to quantify and simulate maintenance choices and their impact on performances [44,73] (Fig. 1B).

Thus to obtain executable patterns from qualitative knowledge (the semantic rules), an extension of BN, the Probabilistic Relational Models (PRM) seem to fit with most of the required modeling needs. PRM integrates similar functionalities to BN plus other extended functionalities. For this reason a recall of BN is presented.

4.2. Recall of Bayesian Networks (BN)

A BN is a directed acyclic graph (DAG) in which the nodes represent the system variables and the arcs symbolize the dependencies or the cause–effect relationships among the variables [30,54]. A BN is defined by a set of nodes and a set of directed arcs. A probability is associated to each state of the node. This distribution of probability is defined *a priori* for a root node and computed by inference for the others.

The computation is based on the probabilities of the parents' states and the Conditional Probability Table (CPT). For instance, let us consider four nodes A, B, C and D; with two states (S_{*1} and S_{*2}); structuring the BN (Fig. 4). The *a priori* probabilities distribution of A are defined in Table 5. The *a priori* probabilities distribution of C are defined in a similar way as the node A. A CPT is associated to the nodes B and C. To show how to define a CPT, an illustration based on the node C is provided. This CPT defines the conditional probabilities $P(C|B)$ attached to node C with a parent B, to define the probabilities distributions over the states of C given the states of B (Table 6).

Therefore, the BN inference computes the marginal distribution $P(C=S_{C1})$:

$$P(C=S_{C1}) = P(C=S_{C1}|B=S_{B1})P(B=S_{B1}) + P(C=S_{C1}|B=S_{B2})P(B=S_{B2}) \quad (2)$$

BN can represent a factorization of a joint probability. For example, the BN in Fig. 4 factorizes the joint probability as shown below (2) [79].

$$P(A, B, C, D) = P(A)P(D)P(B|A,D)P(C|B) \quad (3)$$

BN establishes cause–effect relationships between concepts for modeling their interactions (e.g. the effect of maintenance actions on the system performances [39]. A general inference mechanism that permits the propagation as well as the diagnostic is used to collect and to incorporate the new information (evidences) gathered in a study. The Bayes' theorem is the heart of this mechanism and allows updating a set of events' probabilities according to the

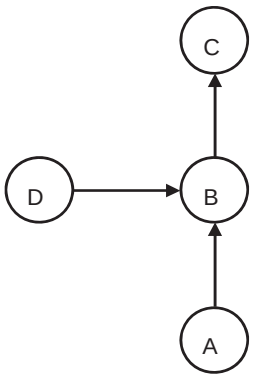


Fig. 4. Basic example of a BN.

Table 5
A priori probabilities of A

A		
	S_{A1}	$P(A=S_{A1})$
	S_{A2}	$P(A=S_{A2})$

Table 6
CPT of the node C given the node B.

		B	
		S_{B1}	S_{B2}
C	S_{C1}	$P(C=S_{C1}\|B=S_{B1})$	$P(C=S_{C1}\|B=S_{B2})$
	S_{C2}	$P(C=S_{C2}\|B=S_{B1})$	$P(C=S_{C2}\|B=S_{B2})$

observed facts and the BN structure. BN, compared to other dependability methods such as Fault Trees (FT) [6], supports multiple failures (multi state variables) representation. This functionality is not supported by FT. In [8,6] present a relevant contribution in which they explain how FT can be translated to BN, maintaining its Boolean behavior.

4.3. Proposition of Probabilistic Relational Model (PRM)

Modeling behaviors and causalities relationships of the MS and of the SoI are complex tasks due to the large number of variables characteristics of the industrial systems. As underlined in the previous section, BN appears to be a solution to model complex systems in the context of this work [76]. Nevertheless, one of the scientific issues related to BN and to Object Oriented Bayesian Networks (OOBN) is that they rise their limits [75]. Indeed BN nor OOBN are not adequate for dealing with very large complex systems [21]. In that way, the PRM is considered as an extended language of OOBN with additional concepts [34,55,64]. It is able to represent the notion of an object and the notion of a class of objects, to inherit attributes and behaviors of classes, to take advantage of the aggregation properties of the set of objects through quantifier attributes, to formalize important types of uncertainties that cannot be accommodated within the framework of traditional BN or OOBN (uncertainty over the set of entities present in a model, and uncertainty about the relationships between these entities) [33]. These capabilities allow knowledge capitalization by the creation of generic classes, which requires only the instantiation to a particular system.

To illustrate a PRM, a representation of a BN and its equivalent PRM are presented in Fig. 5 [67]. Fig. 5(a) shows a BN encoding relations between two different kinds of patterns (variables C_i, on one hand and A_j, B_j, D_j on the other hand). We assume that the conditional probability tables (CPT) associated with variables with the same capital names are identical. When using PRM, the main idea is to abstract each pattern as a generic entity, called a *class*, which encapsulates all the relations between the variables of the pattern.

So, in Fig. 5(b), **X** encapsulates precisely variables A_j, B_j, D_j as well as their probabilistic relations (arcs (A_i, B_i), (B_j, D_j)) and conditional probability distributions. The pattern of variable C_i cannot be directly encapsulated in a class since the CPT of the variable C_i is conditional to variables B_j (e.g. the CPT of C is P($C|B$) according to Fig. 5(a)).

Hence classes must have a mechanism allowing referring to variables outside the class. In PRM, this mechanism is called a *reference slot*. This mechanism allows the creation of some function ρ connecting two classes and allowing both classes to access the variables of the other class. Basically, the idea is to create some pointer ρ allowing a class to extend its scope to attributes in other classes. In that sense, a class can reach the totality of a class' attributes using reference slots. In Fig. 5(b), reference slot gives $\mathbf{X_j}$ access to $\mathbf{Y_i}$'s attributes, e.g., C_i parent is: B_j. Now, as shown in Fig. 5(c), the original BN can be built up from the PRM: it is sufficient to create three instances x_1, x_2 and x_3 class **X** as well as two instances, say y_1 and y_2 of class **Y** and connect them using one edge per reference slot. There is no limit to the number of instance can be referenced (see S in Fig. 5(c)).

To summarize, PRM is defined mainly by classes, attributes of the classes and instances. These elements are explained as follow [19,20,56,67]:

- Classes which represent a common set of attributes of an entire set of similar individuals or objects. In maintenance domain, examples of classes are "components" or "maintenance actions". Moreover, in Fig. 5, two classes **X** and **Y** are shown. Based on the definition given by [67], a class C is defined by a DAG over a set of attributes, i.e. random variables, A(C), a set of references (slots) R(C), and a probability distribution over A(C). Moreover, subclasses represent DAG that are more specific than the superclass (mother class). When a superclass has a subclass, it means that the subclass heritages the same attributes of its superclass and have other specific attributes. For instance, the superclass "equipments" could have a subclass called "pumps" or "valves".
- Attributes define the properties of a class. An attribute has the following characteristics: a type, a name, a list of parent attributes and a CPT. For example, the class "equipment" could have as attributes the "maintenance actions" class. This means that the class equipments depend on the class maintenance actions. Moreover, a list of attributes could be specified.
- Instances are the set of specific individuals or objects of classes. For example, the engine Baudouin 12M26.2P2-002 is a specific individual that is part of the class "equipment". In Fig. 5(c), three instances or specific objects of the class **X** are shown, and two for the class **Y**. Furthermore, once all the instances are created they are linked. This means that each reference of instances has been linked to another reference. This last step of linking the different instances is called system.

Another PRM advantage is its inference aspect. The inference algorithm of PRM allows the computation of large size and complex models. The use of the notion of a class allow the definition of "probabilistic patterns or fragments of the network" through the definition of a family of objects sharing common properties: graph, attributes, references and CPT. From the inference point of view, this capability allows the computation of fragments of the network once and this result could be reused for every instance of the studied system [67].

Furthermore the inference on the PRM is based on the following principles:

- The identification of symmetries and recurrent patterns is performed with an algorithm called Structure Variable Elimination (SVE) which uses the structural information about the

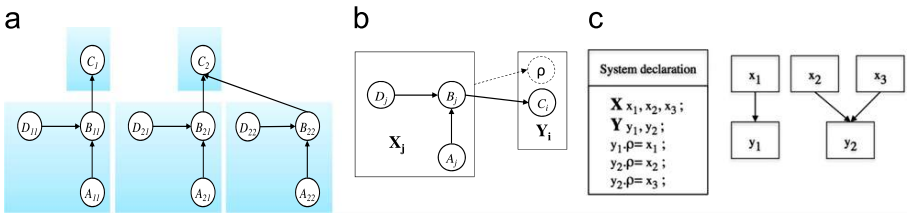


Fig. 5. Representation of a BN as a PRM: analysis of the BN (a) reveals the use of two recurrent patterns, which are confined in two classes (b). Hence, a system equivalent to the BN may be built (c).

PRM to avoid the repeated computations through the elimination of internal nodes at the class level [67].
- The use of the probabilistic "micro-structure" has been possible with the integration of "quantifiers" which ease the quantification of the CPT. In that sense, quantifiers are defined functions, such as logic combinatory functions.
- It is also possible to perform queries by inference in a compiled and specific part of the model. It is not necessary to compute the whole model (described in a language) [19,20,55]. The network is divided into fragments of networks that allow reasonable computation time. This way, the inference could be limited to sub-graphs considered as pertinent to perform the query in the global network. This pertinence is given through conditional independences defined for example by d-separation properties. D-separation defines independency of two variables A and C when they are connected with a third intermediated variable B (either in series, divergence or convergence) (for instance in series in Fig. 4). If the state of the intermediate variable B is known via observation, a conditional independencies is created [30,39], meaning that once B is known, the state of A is independent of the state of D and vice-versa. Thus, once the node is considered as independent it is no longer used for the inference computation.

From the reasons previously detailed (compact representation of knowledge, assessment of the influencing factors in big size models), PRM seems to be a right solution for developing the unified model (kernel of our methodology) needed since the knowledge must be divided into groups of "local knowledge", that could be assembled according to the needs in order to form a whole coherent model.

In relation to "conventional BN", PRM is bringing added value in relation to: modeling power (possibility to develop big-size models), model development (possibility to reuse generic elements stored in library and based on object notion), model parameterization (PRM are integrating quantifiers which facilitates quantification phase).

Within the SKOOB project, a language (SKOOL Language) was created and an inference engine to represent PRM models in order to support PRM functionalities for the representation of large and complex models [63].

4.4. Specification of the SKOOL language: a support language for the PRM

The SKOOL language is based on the syntax of Java language which is one of the more common object-oriented languages used today. The characteristics of SKOOL language[9] are built on the principles of the PRM such as: compilations units like variables, models and classes (declaration of attributes, references, conditional probability table (CPT), specialization, quantifiers or aggregators). For example, the "declaration of a class" (to represent common attributes of a set of objects i.e. every component has an availability) provides reusable probability models and can be applied to many different objects. A class is specified as follow:

```
class Name_of_the_class {
  // Body of the class
}
```

It is possible to specialize a class. One class could have a set of subclasses with more specialized attributes (knowledge specialization). The specialization allows to define top-down concepts. Therefore a general concept is defined as a "Superclass" (a general concept, i.e. a component class) and it is specialized to a specific concept (subclass, i.e. a pump class). The syntax of a specialized class is:

```
class sub_class extends super_class {
}
```

The CPT (e.g. Table 5) in the SKOOL language is written in the following order:

```
[0.9, 0.1, // P(C=SC1|B=SB1), P(C=SC2|B=SB1)
0.2, 0.8] // P(C=SC1|B=SB2), P(C=SC2|B=SB2)
```

There is the possibility to quantify the CPT using aggregation functions. The SKOOL language integrates five aggregation functions: min, max, exists, forall and mean. For example the functions "exists" and "forall" (which correspond to an OR/AND logic functions respectively) take into account two parameters: one list of references' chains and one modality. The resulting value is a boolean value. The syntax is defined as follow:

```
class A {
boolean one_exists=exists([chain_1, chain_2,…],
  one_modality);
}
```

SKOOL language has been used to build generic patterns. In order to receive a better understanding of the skool language, it exists a French tutorial for the Bayesia software (using SKOOB inference engine). It can be also retrieved another open source software called "Enterprise architecture Assessment (EA2T) tool" which could be used to model PRM.

5. Pattern building (Fig. 1B)

Patterns are built based on the dependences described in semantic rules defined in Section 2 (Fig. 1B). Indeed, the knowledge encapsulated within the rules is used to create probabilistic patterns in which (1) variables and main concepts issues of semantic rules represent the classes (or nodes on BN representation) and the arcs represent causality relationships or dependences between concepts (Table 7—Phase 1). Then (2) patterns are assembled. Classes or variables' states are defined by using the dysfunctional knowledge (i.e. FMEA, HAZOP) (Table 7—Phase 2). After (3) the probabilities are determined in the conditional probabilities tables (when the parameter estimation is not possible, the BN quantification is based on the expert judgments) and utility nodes are integrated in order to quantify economical performances (Table 7—Phase 3). The PRM patterns are supported by the SKOOL language. To estimate probabilities distribution, PRM inference is used. However, to explain and to illustrate patterns in this paper, the SKOOL language is compiled and visualized with the BayesiaLab tool (http://www.bayesia.com). (4) These generic patterns (Fig. 1C) could be used during the instantiation phase for creating a global unified model by assembling patterns (Table 7—Phase 4). The compilation offers a best visual representation of the PRM, in the form of Bayesian Networks (as shown in the paper).

5.1. Modeling patterns of the SoI functions (generic simple function) (Table 7—Phase 1)

The semantic rules issued from the SoI and MS analyses emphasize the dependence of the "HD output flow" on the input flows' state (Fig. 6). This relation is considered in the formalization of the PRM classes (allowing to build patterns).

[9] Further details on the SKOOL language are provided on the URL: http://skoob.lip6.fr/doku.php?id=public:texte_anglais_de_presentation.

This step requires the formalization of the generic classes of variables such as the input and output flows of a function. Within a PRM class, dependences with concepts of the SoI are defined. For example, the concept of flow and its relationships is extracted from semantic rules. This concept is used to create the "flow class". This class allows representing the different types of flows: HD, KHD, WD and AD. Within the SKOOL language, it is defined as:

```
class Flow{
Typestate state{ [0.99,0.01] };// Basic type for Boolean flow
  description
}
```

Then this class can be specialized into "output flow class" in order to represent all output flows of a function such as AD, HD and RWD (report on the function state in relation to WD flow) for example (Fig. 6). As shown in Fig. 6, the output flow class is created using the same semantic rule defined on the functioning model of the SoI. The output flow depends on the state of the input flows of the function and on the state of the support. Fig. 7 illustrates the coding rules from SADT function "to transform input flow into output flow" and the associated semantic rules to the SKOOL language as well as the resulting BN. Based on these dependences relations, the input flow becomes a root class called "flow". This class could be later specialized as an HD flow, AD flow, etc. On the other side the output flows are integrated in the "output flow class" as a flow with other dependencies (e.g. on the input flows and the state of the support). This pattern should be used for every elementary function of the SoI.

Table 7
Phases to build PRM-patterns.

Phase 1	1.a. SoI modeling pattern 1.b. MS modeling patterns Initial availability modeling patterns Modified availability modeling patterns Operational availability modeling patterns Environmental availability modeling patterns
Phase 2	2.a. Pattern assembly 2.b. Classes' states definition.
Phase 3	3.a. Definition of the conditional probabilities for the CPT of the classes 3.b. Integration of utility nodes to evaluate the impact of maintenance strategies on financial SoI performances
Phase 4	Patterns instantiation into a specific model

5.2. MS modeling patterns (generic complex function) (Table 7—Phase 1)

The MS patterns are built using the same modeling methodology applied to the SoI. The main MS rule identified in Table 3 describes that the availability of the support depends on the maintenance plan, the resources (i.e. the availability of spare parts, tools, etc.), the staff (i.e. its effectiveness) and its surrounding environment. Using this same reasoning logic, [49] shows a generic way of the effectiveness of an action. Knowing that, the effectiveness depends on the staff, on the resources quality and on the quality of procedures.

Thus this MS pattern is a complex function and is built from four patterns functions. The first pattern allows calculating the "initial availability" (A) from the maintenance plan. The second pattern computes the "modified availability" (B) from the "initial availability". This pattern takes into account the impact of logistics on the "modified availability" of the support. The third pattern estimates the "operational availability" (C) from the "modified availability". This pattern considers the impact of the human effectiveness on the "operational availability". The last pattern computes the "environmental availability" (D) from the "operational availability" by integrating the impact of the environment on the availability of the support [28]. The "environmental availability" becomes an input flow of the SoI pattern as the "support of a function" of the SoI (Fig. 2). Based on the necessary flows (maintenance plan, logistic effectiveness and human effectiveness), different MS patterns were created allowing to assess the "component availability" (Fig. 8).

(A) For example, the "initial availability" (support.initial_availability) pattern (Fig. 8A) is created based on the following steps: (1) consideration of maintenance actions types and its restoration degree for determining the time and the effectiveness of the maintenance actions leading to define a "Maintenance Actions" variable. (2) Afterwards, condition-based and predictive maintenance need a reliable monitoring system. This variable is integrated into the pattern as the class "monitoring system's reliability" in which false alarms and non-detection are considered. (3) The "monitoring system's reliability" class impacts the maintenance actions planned. This effect is shown within the "modified maintenance actions" class.

(B) To create the logistic pattern, semantic rules specify that if resources are not available, maintenance actions cannot be executed or they will wait until resources are available. Thus the MDT will increase and the availability of the component will decrease. In that sense, another pattern integrates (1) all

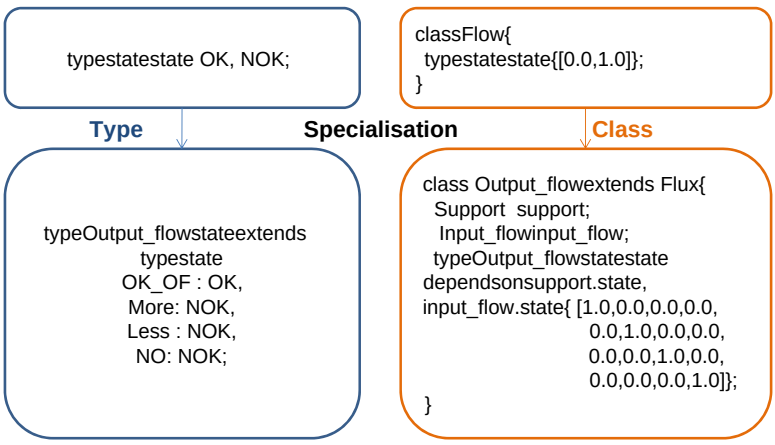


Fig. 6. Classes' specialization within the PRM.

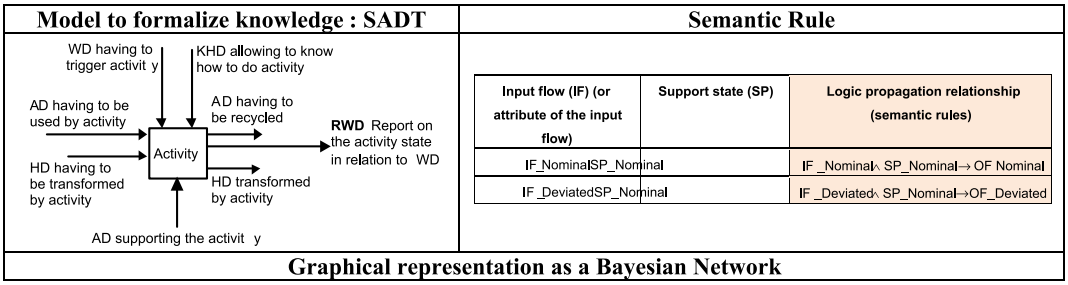


Fig. 7. Generic pattern of SoI functions formalization.

material necessary to perform a maintenance action such as "tools", "staff" and "spare parts". (2) Then the logistic elements are grouped together into a class called "maintenance logistic effectiveness" (Fig. 8B). This class impacts the component availability based on the resources availability. This way, this second pattern allows to compute the "modified availability" (support.modified_availability).

(C) The impacts of other enabling systems of the MS are considered. As specified on semantic rules maintenance operators' performances impact the availability of the component. To consider the impact of the organizational context on the human effectiveness, the approach developed by [39] was taken into account. When the staff is not effectiveness, then component availability is impacted as well (Fig. 8C). This pattern integrates (1) the POFs (organizational context of the operators). (2) Then the action of operators will impact different phases of the maintenance actions, such as the "preparation", the "execution" and the "closure". (3) Finally this pattern considers the impact of the "human effectiveness" on the "operational availability" (support.operational_availability).

(D) At last, a pattern about the "environmental availability" (support.environmental_availability) is proposed (Fig. 8D). Actually components are impacted by the operational conditions they are surrounded. The operational profile, the environmental conditions and so on may impact the evolution of degradation mechanisms which affects directly the MUT and thus the availability of the component. In this way, this pattern integrates the impact of the "environment" into the support's availability.

In summary, generic patterns of the maintenance architecture are built in a modular way in order to unify different types of knowledge needed to evaluate some KPI such as the availability of the component and of the SoI. For modeling and assessing maintenance strategies, it is not necessary to use all patterns. If data is not available or if it is not critical, it is possible to eliminate one or more of the patterns. This kind of structure eases

and guide global modeling of a specific application by capitalizing knowledge and pattern re-exploitation of a model.

5.3. Patterns assembly (Table 7—Phase 2)

To assemble patterns of the SoI and of the MS it is necessary to identify a common element that links both systems. The common element is the component that supports a function of the SoI. In this way the "environmental availability" becomes an input flow of the elementary function of the SoI (Fig. 9).

To connect the different instantiated patterns of the SoI, functions are linked through their flow exchanges. In that sense, a semantic rule establishes that the output flow of an upstream function becomes the input flow of the downstream function (Fig. 9).

5.4. Definition of the states of PRM-classes (Table 7—Phase 2)

The PRM patterns, presented in the previous section, have to be completed with the information concerning variables modalities and with associated quantification methods for probabilistic computations. In that way, generic modalities and quantification methods have been defined for each group of variables.

The states of input and output classes are defined on the malfunctioning system analyses, such as failure modes or flow deviations (FMEA or HAZOP methods). For example, one of the attributes of a "flow" could be its "flow rate". The deviations of the "flow rate" attribute (identified in the HAZOP) could be: more, less or no (Fig. 10). Another example could be shown for the monitoring system of the MS. The main attribute of the monitoring system is its reliability. The nominal state is the "detection" of a degradation level and the deviations of this attribute are the "false alarms" and the "non-detection".

Using this reasoning the states of the classes are defined as follow:

- For the "Maintenance Actions" and the "Modified Maintenance Actions" the states are: "Minimal-Corrective" (MC), "Perfect-Corrective" (PC), "Perfect-Time-based maintenance" (PTb), "Imperfect-Time-based maintenance" (ITb), "Minimal-Time-based maintenance" (MTb), "Perfect-Condition-based maintenance" (PCb), "Imperfect-Condition-based maintenance" (ICb) and "Minimal-Condition-based maintenance" (MCb). It means that planned maintenance actions are either after a failure with different restoration degrees (MC and PC) either before the failure without knowing the real state of the support (PTb, ITb and MTb) or either before reaching a degradation level that leads to the failure (PCb, ICb and MCb).
- "Monitoring system's reliability": "Detection" (D) and "Non-detection" (ND) and "False Alarms" (FA). The monitoring system can reveal a failure (D), can fail to reveal it (ND) or can point out the presence of failure when there is no failure (FA).
- "Environment": "Nominal" (N) and "Non-nominal" (NN). It means that the operational conditions are those considered by the manufacturer (N) or they overpass the operational conditions considered by the manufacturer (NN).
- POF: "Absent" (A) and "Present" (P). It means that the pathogenic feature of the considered organizational factors (A) has not been proved, (P) has been proved.
- "Human effectiveness" and "maintenance logistic effectiveness": "Effective" (E) and "Ineffective" (I). It means that the considered variable (E) fulfils the function for which it has been implemented; (I) does not fulfill this function.
- "Initial availability", "modified availability", "operational availability" and "environmental availability": "Available" (A) or "Unavailable" (U). It means that the component is in a functioning state (A) or in a non-functioning state (U).
- For HD flows and AD flows: The states of the flow are specified within the HAZOP study as the deviation of flow properties. For the SoI flows, there could be several states for the HD flow/AD flow, such as "more temperature" or "less temperature". Nonetheless, for the MS flows such as the spare parts or staff (AD flows), two states are considered: Available (A) or Unavailable (U).
- For RWD flow: The states of this informational flow are grouped into two macro-states: "OK" which means that the function was performed as expected and "NOK" which means that the function was not performed as expected.

5.5. Model quantification (Table 7—Phase 3a)

Once the model is built and the states of the classes are defined, then a quantification phase of the parameters of the classes is required. This quantification is based on logic combinatory, historical data and on the methods of improving/aggravation factors such as the noisy-or and noisy-and functions. The SKOOL language provides some functions such as the "exist/forall functions" which are equivalent to an "OR/AND logic functions" respectively. These functions fulfill automatically the CPT in order to reduce the modeling efforts. In that sense, the proposed patterns have predefined quantification functions. However, these functions could be changed if the modeler has additional knowledge/data.

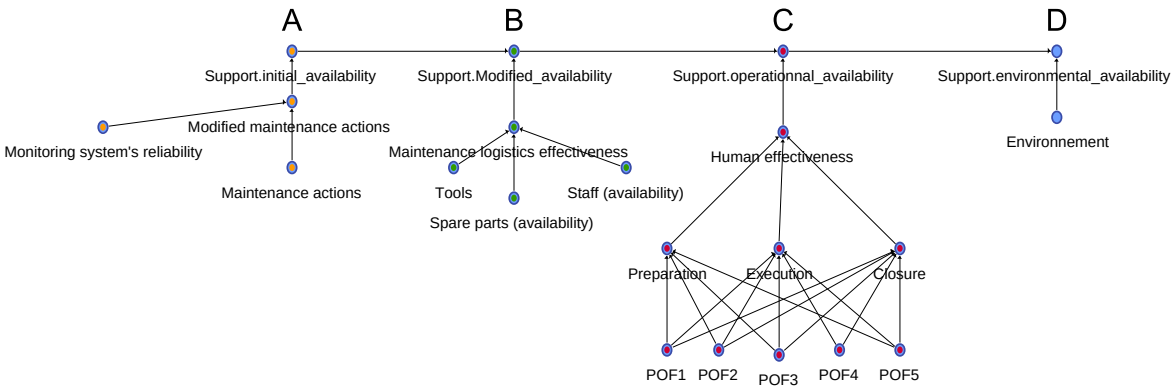


Fig. 8. Generic patterns of the MS.

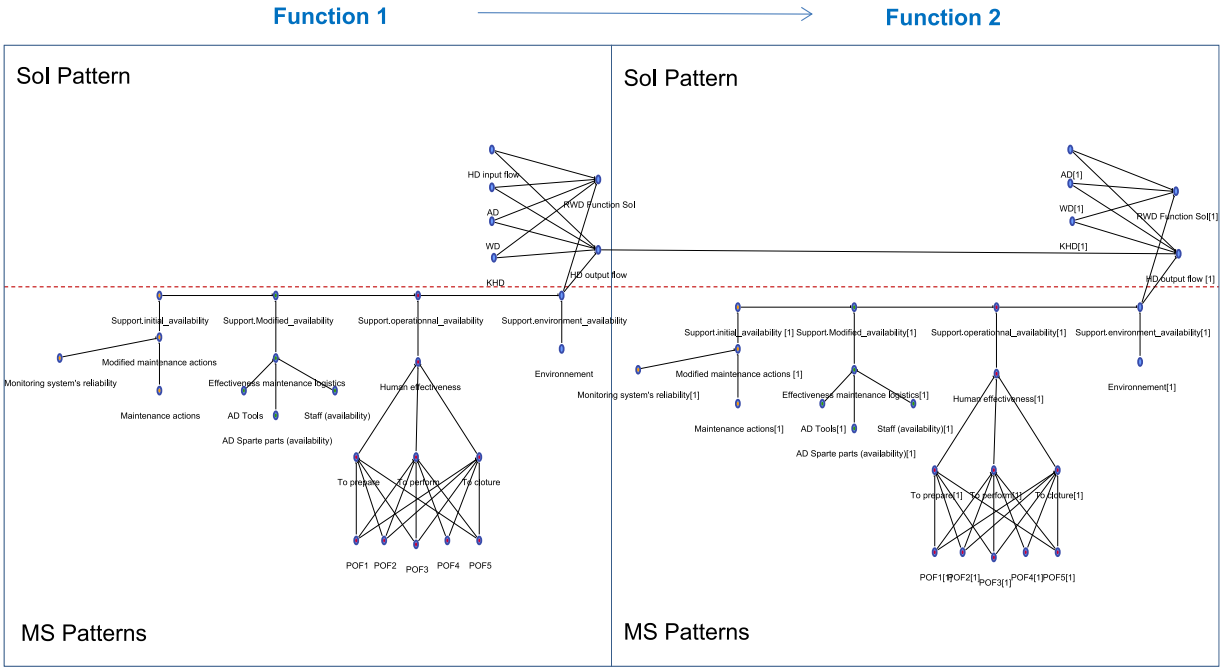


Fig. 9. SoI and MS patterns assembled at the same abstraction level.

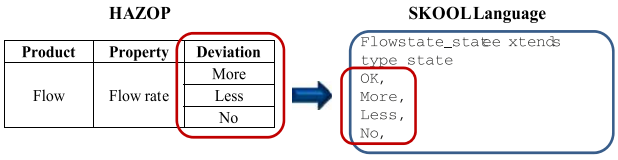


Fig. 10. Definition of the states of PRM-classes from an HAZOP study.

This model allow to forecast the impact of maintenance logistic choices, human resources policies and maintenance actions plan on the system performances such as the availability of the system. Additionally PRM also allow to perform diagnostic to identify the variable(s) that is (are) more probable to cause performances deviations in order to take corrective action and to improve global performances.

This way it is possible to represent the multiple functions of a real industrial system. However, one of the most important performances is the financial performances. For this reason, this aspect is integrated into the proposed model.

5.6. Proposition of MS impact on financial SoI performances (Table 7—Phase 3b)

In this section the financial impacts of maintenance decisions are taken into account within a maintenance strategies assessment model. In that sense "utility nodes" are integrated allowing to estimate a "mean value" of the cost function based on the probability that the different scenarios occur (variables' states) [77].

A maintenance costs function was proposed based on the contributions of different authors [12,44]. This function integrates the total incomes as well the total costs related to the production and maintenance activities. The function is defined as follow:

$$P = \text{I}–\text{FC}–\text{PC}–\text{MC}–\text{LC}–\text{SC}–\text{DC} \quad (4)$$

where P: profit; I: incomes; FC: fixed costs; PC: production costs; MC: maintenance costs; LC: logistic costs; SC: staff costs; DC: down time costs.

To take into account these elements on the proposed model, the financial elements depend on:

- Incomes (I): Represent the total incomes from products sales. Based on the proposition of [44], this utility node depends on the state of node "RWD final system function" (probability to perform the function). This node also takes into account costs related to the unavailability of the system.
- Production costs (PC): This node integrates costs related to the raw material and the energy expenses. It depends on the state of the final flow represented by the node "RWD final system function".
- Maintenance costs (MC): This node considers the costs associated to the spare parts and energy required to satisfy MS requirements. It depends on the state of the node "Modified maintenance actions".
- Logistic costs (LC): This node takes into account storing and transportation costs of materials. It depends on the nodes "Tools" and "Spare parts",
- Staff costs (SC): These costs are related to the availability of the staff. It depends on the node "Staff availability".
- Down time costs (DC): It considers the costs related to the unavailability of the system. It depends on the "Modified maintenance actions" node.
- Fixed costs (FC): This costs are independent of the production activities and are represented by the administrative costs, rents of facilities, etc. Since it is independent of any activity, this node does not depend on any node.

If several functions are defined, there will be only one node that groups the LC and the SC costs associated to these functions. This approach does not represent the real costs generated by production and maintenance activities because within the model, costs are estimated using probabilities of the different and possible scenarios. These utility functions allow the estimation of the mathematical mean value of costs based on the different probabilities of each state [77]. Nonetheless this function allows comparisons of the different maintenance strategies by estimating financial trends.

6. Case study (Fig. 1C)

The feasibility of the proposed methodology is shown with an instantiation phase (Fig. 1C) (Table 7—Phase 4) applied to a real harvest production system (SoI). One of the SoI requirements is to choose maintenance strategies to minimize harvest microbiological pollution. The production line is composed mainly by a tank and a charging line (Fig. 11).

The global SoI function is to produce harvest. The multi-point of view modeling is applied to this system for identifying the main items of the instantiation phase. The functional analysis of the SoI involves five abstraction levels. The last level involves 65 elementary functions thus the "SoI function pattern" is instantiated 65 times as well. Each elementary function is supported by a component (65 components). Among the components there are valves, joints, heat exchanger, sensors, PLC, etc. For each support, MS patterns are instantiated. For example, Fig. 12 shows the instantiation phase of the "initial availability pattern" for two valves. This pattern integrates all maintenance actions to maintain valve such as corrective and preventive actions to face degradation of supports. Also maintenance costs are integrated into the model. It also shows a part of the integration of the utility nodes to represent the maintenance costs of some supports (components).

As explained before all maintenance actions could be seen as a maintenance function that needs tools, staffs and spare parts to be performed. To represent how maintenance logistic choices such as the stock level, ordering policies, etc. impact MS performances, tools, spare parts, staffs, etc. are integrated into the model (i.e. modified availability pattern). This pattern is instantiated only once into the PRM model. This modeling choice is selected because the same logistics supports the MS. Thus, logistics is not independent, if logistics is ineffective for one support it will also be ineffective for the other supports too since it' is the same logistics system (e.g. same tools) (Fig. 13).

Then to study the impact of operators' performances into the supports' performances, the "operational availability" pattern (for human effectiveness impact) was integrated once into the model (Fig. 14).

Finally, the environment impacts the evolution of degradation mechanisms leading to instantiate the "environmental availability" pattern for which two environment types were identified: an "aggressive environment" for three valves that are more required than the average requirements on the cleaning and sterilization phases and a "regular environment" for the other components (Fig. 15).

All these instantiated patterns are assembled to obtain a global model that integrates the impact of the different enabling systems into the SoI performances (Fig. 16). The model contains the four intermediate availabilities issues of the MS-enabling system interactions. This way it is possible to estimate the "environmental availability" of every support. Also the model integrates the impact of this availability on each function of the SoI.

6.1. Parameters of the production harvest model

After patterns instantiation, the resulting global unified model cannot be supported by BayesiaLab tool since there' is an "out of memory error" due to the big size of the model. However the Bayesia PRM tool, thanks to their inference algorithms, allows the computation of large size models. The global model is parameterized using data from the CMMS (Computerized Maintenance Management System) of the plant and expert judgments. As defined in Section 1, it is required to forecast some KPI such as the availability and financial performances at a system level to assess maintenance strategies. In that sense, three scenarios are shown about the maintenance of valves which are critical components of the SoI. These scenarios allow comparing by simulation what are the most appropriated maintenance strategies for valves. The initial values of the CPT are defined in Table 8. On the basis of the historical data stored in the CMMS, it was selected a Weibull distribution as failure distribution of the valves, with scale parameter $\beta=3.5$ and shape parameter $\alpha=9900$.

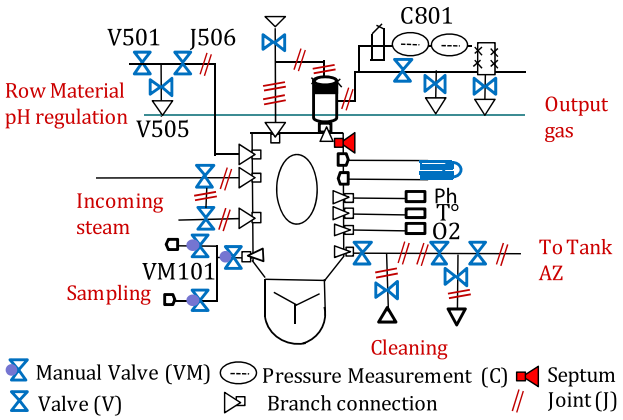


Fig. 11. Part of the production harvest system.

6.2. Contribution to the verification and validation of the model

The resulting model needs to be now verified and validated in order to conclude on the quality of the proposed model.

The verification is the confirmation by examination and provision of objective evidence that the specific requirements have been fulfilled. The verification phase requires answering: Have the appropriate model been built [27].

To contribute to the verification of the proposed model, this one is based on the principles of the system theory. This fact means that the model is based on semantic rules (issues of the knowledge multi-point of view representation of the system theory) to build dependences relationships between the PRM patterns.

A second step to contribute to the verification of the model is to analyze the "*a priori* probabilities distributions". This verification could help to identify the following items:

- Modeling errors such as non-reachable modalities due to errors in the probabilities definition or to the non-respect of constraints,
- Illogic *a priori* distributions.

For example, in this case, it is possible to verify that when an observation is added on the "maintenance logistic effectiveness" variable and this one becomes "ineffective", the availability of the last function of the SoI "to transfer harvest" turns into 0% (Fig. 17). This result corresponds to the expected behavior. If there is a total ineffective logistics, components would not be repaired when they failed because of lacks of spare parts, tools, etc. and thus the SoI would be unavailable. Moreover if an observation is added about the non-existence of input flow (NOT flow rate ingredient), there should not be any output flow rate (Fig. 18).

In addition, a contribution to validation was performed. The validation is the confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled. Validation is related to the question: Have the model been built right? [27].

One of the techniques used was the "independent verification and validation". This technique uses a third party to decide about the validity of the model. The third party was independent to the team that developed the model and it worked for the production harvest system. The third party entity tests the model to compare

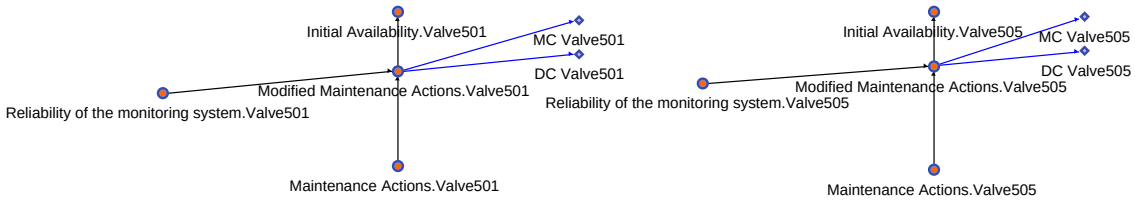


Fig. 12. "Initial Availability" pattern instantiation to valves.

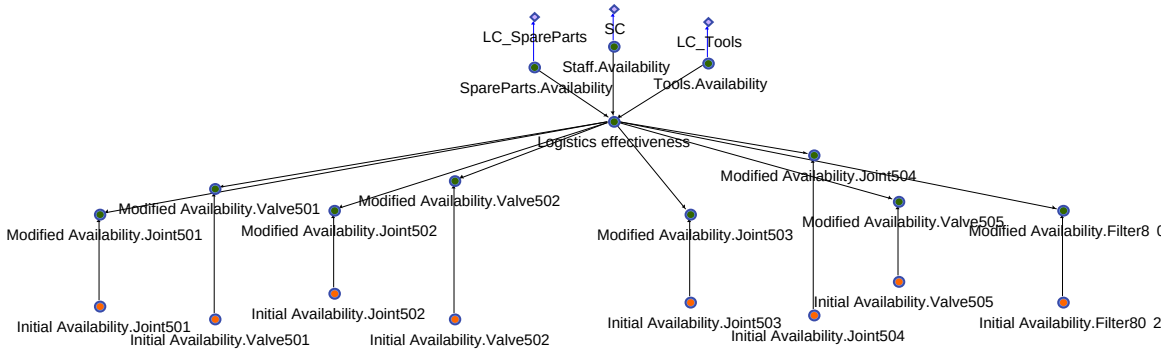


Fig. 13. "Modified Availability" pattern instantiation to different supports.

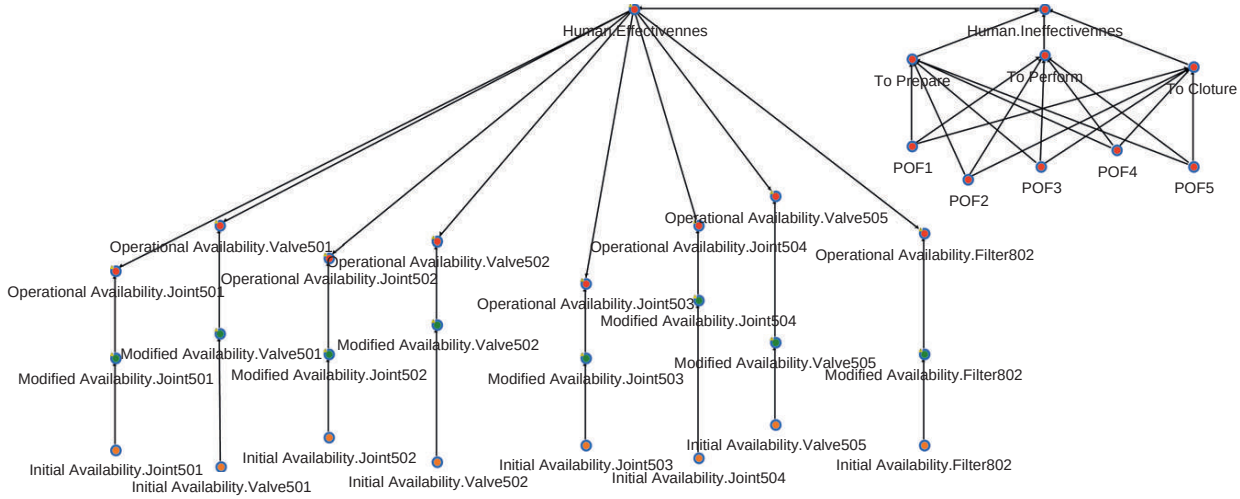


Fig. 14. "Operational Availability" pattern instantiation to different supports.

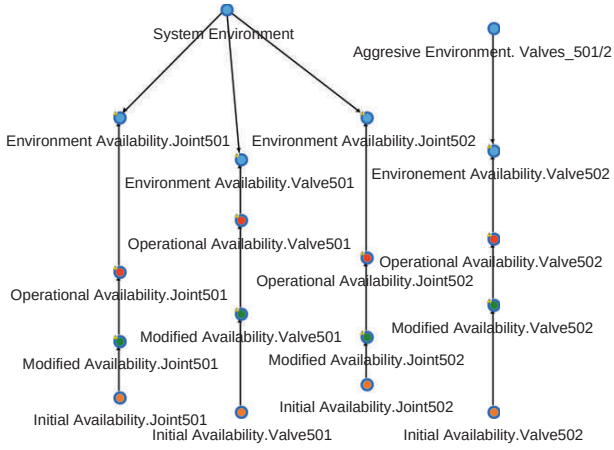


Fig. 15. Instantiated "Environmental Availability" pattern.

different simulations scenarios. This approach helps to the credibility of the model [59].

Moreover, a sensibility analysis was used to verify the factors that have a highest influence in the model [49]. Indeed [58] presents a methodology to perform sensibility analysis for BN. This technique aims to "measure the sensibility of changes in probabilities of query nodes when parameters and inputs are changed". The same methodology is applied with PRM model.

A sensibility analysis was performed on the output variable "harvest flow rate". This technique allows to show in a graphical way the impact of the different variables of the network into each of the states of the chosen variable. The variation of each state is shown based on the variation from 0% to 100% of the values of the parent nodes (direct or indirect parents). This way it is possible to observe how "a posteriori probability distribution" of the "harvest flow rate" variable changes under different conditions [58]. Fig. 19 shows the variation of the state "OK" of the variable "harvest flow rate" based on the variation of each of its parents.

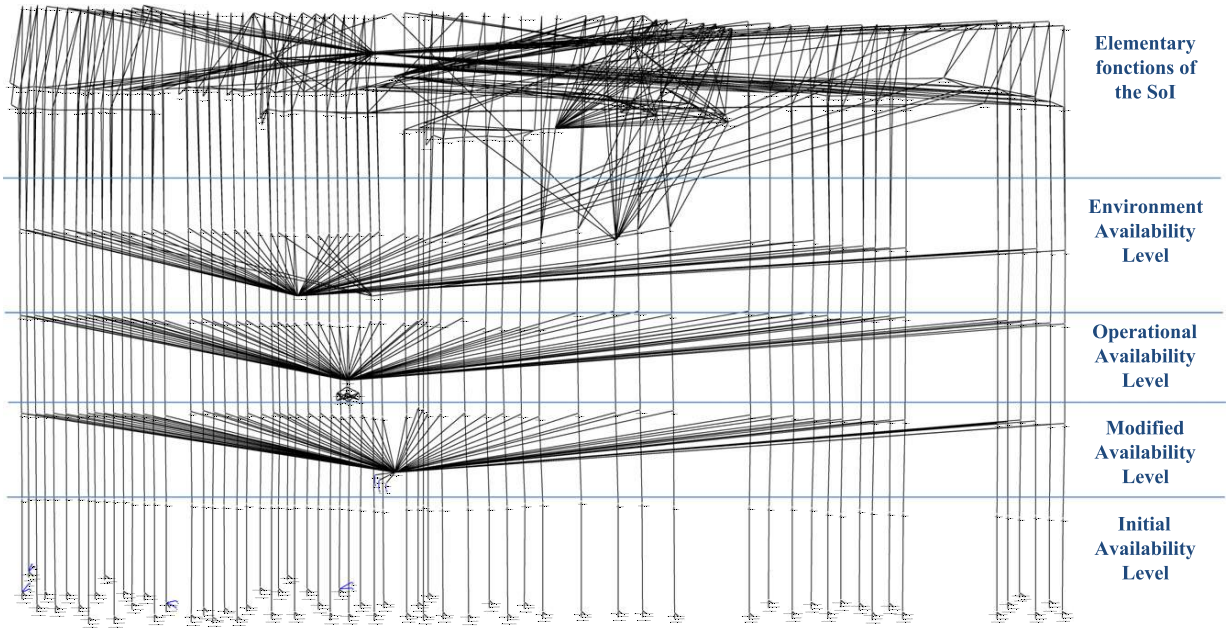


Fig. 16. Global Harvest Production System and its Maintenance System PRM-Model. (65 components, approx. 600 nodes).

Table 8
Model parameters.

Variable	Modes	Scenario 1 corrective maintenance	Scenario 2 time-based maintenance	Scenario 3 condition-based maintenance
Availability of resources	Available	99.91	99.91	99.91
	Non-available	0.09	0.09	0.09
Availability of the personnel	Available	99.91	99.91	99.91
	Non-available	0.09	0.09	0.09
Monitoring system's reliability	Detection	96	96	96
	Non-detection	1	1	1
	False alarm	3	3	3
POFs	Absent	100	100	100
	Present	0	0	0
Maintenance action	Perfect-corrective	100	5	0
	Minimal-corrective	0	0	0
	Perfect time-based	0	95	0
	Imperfect time-based	0	0	0
	Perfect condition-based	0	0	100
	Imperfect condition-based	0		0
	Minimal condition-based	0	0	0

In Fig. 19 it is possible to underline the fact that the POFs nodes impact slightly the variable "harvest flow rate". However, this analysis also shows that when the supports of the process are available, the "harvest flow rate" remains in a nominal state.

Once the different validation and verification phases are performed, it is possible to conclude about a satisfying confidence degree of the model to represent MS and SoI. Thus simulations can be done.

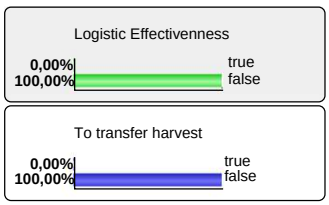


Fig. 17. *A priori* probability distribution analysis of the variable "logistic effectiveness.

6.3. Simulations

To simulate maintenance strategies assessment, different scenarios are considered. In the simulation mode, these scenarios show the impact of different maintenance strategies on the valve such as corrective, time-based at different intervention frequencies and condition-based on SoI performances. To perform simulations the software Bayesia (SKOOB inference engine) was used and parameters (i.e. conditional probabilities) of patterns were changed according to each scenario. The initial values of the CPT were defined previously in Table 8.

Fig. 18. *A priori* probability distribution analysis of the variable "Flow rate of the initial ingredient F0".

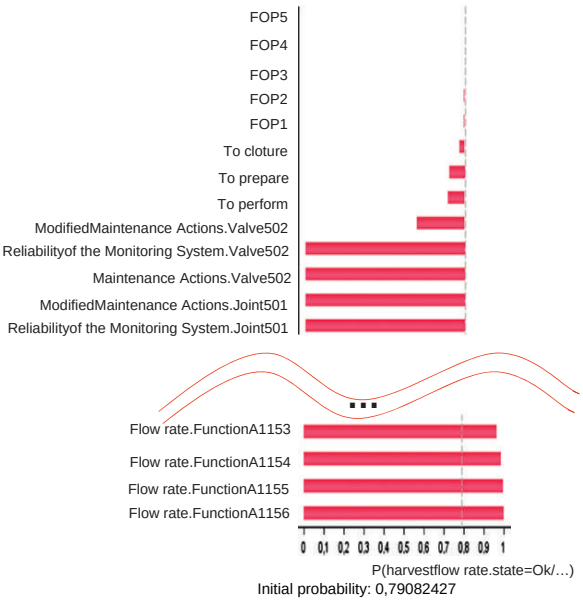


Fig. 19. Sensibility Analysis of the variable "harvest flow rate" in the modality "OK".

On the basis of model simulation results, Figs. 20 and 21 underline the performances of the SoI in relation to availability and financial items. In this scenario, it is considered that other supports of the plant follow a corrective maintenance strategy.

The results show that the performances of the SoI are optimized when the supports follow a condition-based maintenance strategy. Nonetheless, it can be observed that corrective maintenance provides sometimes better SoI availability than time-based maintenance done at a low frequency. This result can be explained by the fact that periodic actions at a low frequency do not prevent failure apparition (too late) and they penalized availability by performing an ineffective preventive action. In this case, the availability calculated every 16,000 h is similar to the one obtained with corrective actions. Moreover time-based maintenance with too high frequency (i.e. every 3000 h) produces important maintenance costs. However these costs are offset with the obtained SoI availability.

For the time-based strategy, the best availability performances were obtained around 8500 h but the best financial ones were obtained with 3000 h. It is explained due to the high penalization costs when valve fails since if a valve leaks, production could be polluted and thus rejected. At 8500 h, the component reliability decreases compared to the valve reliability at 3000 h. With this scenario, it was also tested, for condition-based strategies, the sensibility of SoI performances to the reliability of the monitoring system. When a perfect detection is considered, the availability of the SoI is 0.6379. But if there is a probability of 0.96 to detect the degradation level and 0.04 the probability to produce false alarms,

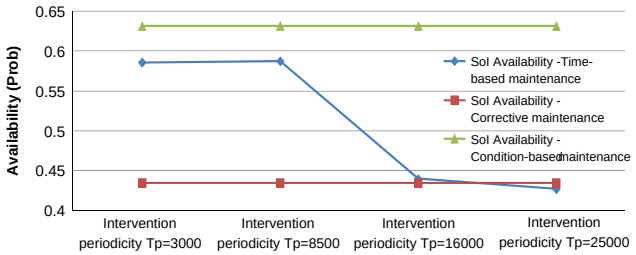


Fig. 20. Availability of the SoI after different maintenance strategies applied to valves.

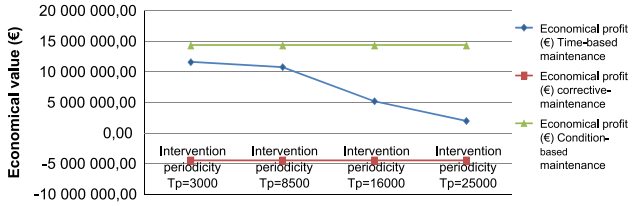


Fig. 21. Financial performances of the SoI after different maintenance strategies applied to valves.

the availability of the SoI is going to 0.6316. In this particular case, the reliability of the monitoring system does not have a big impact on the SoI performances. However it is only considered the effect of false alarms. If the effect of non-detection is taking into account, the impact should be higher on SoI performances. Finally a diagnostic phase based on PRM inference algorithms could be analyzed to identify the most probable causes related to deviations.

7. Conclusions

In this paper a methodology based on system engineering thinking is proposed. This methodology integrates the impact of the MS into the SoI performances. This methodology is based on the formalization of the main concepts both of the SoI and the MS in a generic way. The main concepts are linked via logical relationships or semantic rules. This approach is innovative because it leads to create semantic rules independent of conditions and hypotheses related to the classical dependability model. Moreover this methodology allows the integration of semantic related to maintenance strategies assessment to dependability models and more specifically to PRM formalism. These rules guide the model development in order to guarantee the model coherence.

In that sense, semantic rules lead to define PRM-based generic and probabilistic patterns. The difference of PRM, in comparison with other classical methods is its polyvalence. It allows dealing with issues such as the development of large size model (multi-component systems), generic elements reusing, the integration of quantifiers, performing prediction and diagnosis, integrating feedback experience as well as model updating. The graphical representation in BN is interesting since the model complexity is understandable in a single view. Besides PRM allow to compute large size models which cannot be computed with classical BN. PRM computes the distribution probabilities within few seconds thanks to their inference algorithms. This is an important feature to perform several simulations to assess, for example, different maintenance strategies choices.

In that sense, PRM-patterns were built to represent the main aspects of the SoI and the MS. Four patterns (initial, modified, operational and environmental availability) were proposed to represent the interaction of the MS with its enabling systems.

Other patterns were proposed to integrate the impact of maintenance decisions on the SoI performances. Furthermore, other factors were incorporated in the model such as "financial point of view". Financial assessment was possible with the integration of utility nodes within the model. This way, maintenance assessment was based on multi-performances estimation.

These patterns are stored in library in the forms of COTS (components off the shelf; easing pattern re-exploitation) and can be used, by instantiation, to a specific industrial case (SoI and MS). The instantiation of the generic patterns allow to build a global unified model. This model supports simulation to quantify performances in the decision making process with regards to production/maintenance optimization. The experimentation on a real system has been shown while providing the feasibility and the added value of this methodology. In addition, a verification and validation phase was performed in accordance with the system reality.

However, further developments should be done such as the adding of others MS patterns (i.e. subcontracting).

Furthermore, since this approach deals with probabilities, usually they are considered as known perfectly (all the information on the behavior of a system and its component). However, this condition is rarely fulfilled [69]. For this reason, another interesting issue is the quantification of the imprecision within the parameters and the knowledge of the model (uncertainty). The theory of Dempster Shafer proposes a relevant formalism, and the evidential networks applied in reliability by [61] are suitable for decision making, considering the imprecision on the utility computation. In that sense, [16] deals with the belief function networks. They proposed to keep the structure of the network in order to manipulate the uncertain knowledge. The uncertain knowledge is related to the epistemic uncertainty (e.g. unknown probabilities). This approach allows the computation of interval of probabilities based on the uncertain knowledge. Another issue is the integration of dynamics in the unified model in order to take into account the evolution of some phenomenon such as the evolution of the operational conditions or the evolution of the degradation of a component [5,7,75].

Acknowledgment

The authors wish to express their gratitude to the French National Research Agency (ANR) for the financial support of the Structuring Knowledge with Object Oriented Bayesian nets (SKOOB) project. Ref. ANR PROJET 07 TLOG 021 (http://skoob.lip6.fr). Special thanks are also paid to all the partners of this project who contributed in development of the proposed methodology as well as in the development of the inference algorithm for the PRM.

References

[1] Alexander C, Ishikawa S, Silverstein M, Jacobson M, Fiksdahl-King I, Angel S. A pattern language. New York: Oxford University Press; 1977.
[2] Alsyouf I. The role of maintenance in improving companies' productivity and profitability. International Journal of Production Economics 2007;105:70–8.
[3] Barros A, Bérenguer C, Grall A. A maintenance policy for two-unit parallel systems based on imperfect monitoring information. Reliability Engineering and System Safety 2009;91(2006):131–6.
[4] Bartholomew-Biggs M, Zuo M, Li X. Modelling and optimizing sequential imperfect preventive maintenance. Reliability Engineering and System Safety 2009;94:53–62.
[5] Ben Salem A, Muller A, Weber P. Dynamic Bayesian Networks in system reliability analysis. In: Proceedings of 6th IFAC symposium on fault detection, supervision and safety of technical processes. Beijing (PR China); 2006. p. 481–6 [accessed 30.08.06].
[6] Bobbio A, Portinale L, Minichino M, Ciancamerla E. Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. Reliability Engineering and System Safety 2001;71(3):249–60.
[7] Boudali H, Dugan JB. A discrete-time Bayesian network reliability modeling and analysis framework. Reliability Engineering and System Safety 2005;87(3):337–49.
[8] Castillo E, Solares C, Gomez P. Tail uncertainty analysis in complex systems. Artificial Intelligence 1997;96:395–419.
[10] Chelbi A, Ait-Kadi D. Inspection strategies for randomly failing systems. Handbook of Maintenance Management and Engineering. London: Springer Verlag London Limited.; 2009.
[11] Cho D, Parlar M. A survey of maintenance models for multi-unit systems. European Journal of Operational Research 1991;51:1–23.
[12] Crespo-Márquez A. The maintenance management framework: models and methods for complex systems maintenance. Springer series in reliability engineering.Springer; 2008 ISBN: 10:1846288207.
[13] Delmotte F. A socio-technical framework for the integration of human and organizational factors in project management and risk analysis. Master of science, Faculty of the Virginia Polytechnic Institute and State University.
[14] Dutuit Y, Chatelet E, Signoret JP, Thomas P. Dependability modelling and evaluation by using stochastic Petri nets: application to two test cases. Reliability Engineering and System Safety 1997;55:117–24.
[15] EN 13306. European standard. Maintenance terminology. Paris: Association Française de Normalisation (AFNOR); 2001.
[16] Fallet G, Duval C, Weber P, Simon C. Characterization and propagation of uncertainties in complex socio-technical system risk analyses. In:Proceedings of 1st international workshop on the theory of belief functions. Brest (France); 2010.
[17] Flacke-Vordos N, Bellou A. Use of Bayesian net tools in acute coronary syndromes. Paper presented at the European Society of Emergency Medicine Congress EuSEM2008, Munich, Allemagne; 2008.
[18] Fouladirad M, Grall A, Dieulle L. On the use of on-line detection for maintenance of gradually deteriorating systems. Reliability Engineering and System Safety 2008;93:1814–20.
[19] Getoor L, Friedman N, Koller D, Pfeffer A, Taskar B. Probabilistic relational models. In: Getoor L, Taskar B, editors. An introduction to statistical relational learning. MIT Press; 2007.
[20] Getoor Lise, Friedman Nir, Koller Daphne, Pfeffer Avi, Taskar Ben. Probabilistic relational models. In: Introduction to statistical relational learning. Cambridge: MIT Press; 2007. p. 129–74 [chapter 5].
[21] Gonzales C, Wuillemin PH. PRM inference using Jaffray & Faÿ's local conditioning. Theory and decision, vol. 71. Springer; 2011 p. 33–62.
[22] Gürler, Kaya. A maintenance policy for a system with multi-state components approximate solution. Reliability Engineering and System Safety 2002;76:117–27.
[23] Ho-Joon Sung. Optimal maintenance of a multi-unit system under dependencies. PhD thesis in the school of aerospace engineering georgia institute of technology; 2008.
[24] Hoyland A, Rausand M. System reliability theory: models and statistical methods. John Wiley & Sons, Inc; 1994.
[25] IEC/ISO62264-1. Enterprise-control system integration—part 1: models and terminology. Edition ISO; 2003.
[26] INCOSE. International Council on Systems Engineering. Systems engineering handbook, vol. 3.2. INCOSE-TP-2003-002-03.2; 2010.
[27] ISO 8402. Quality management and quality assurance. Edition ISO; 1994.
[28] Iung B, Monnin M, Voisin A, Cocheteux P, Levrat E. Degradation state model-based prognosis for proactively maintaining product performance. CIRP Annals—Manufacturing Technology 2008;57(1):49–52.
[29] Iung B, Veron M, Suhner MC, Muller A. Integration of maintenance strategies into prognosis process to decision-making aid on system operation. CIRP Annals—Manufacturing Technology 2005;54/1:5–8.
[30] Jensen FV. An introduction to Bayesian networks. London (UK): Editions UCL Press; 1996.
[31] Kim MC, Seong PH, Hollnagel E. A probabilistic approach for determining the control mode in CREAM. Reliability Engineering and System Safety 2006;91(2):191–9.
[32] Kleindorfer PR, Singhal K, Van Wassenhove LN. Sustainable operations management. Production and Operations Management—Winter 2005;14(4):482–92.
[33] Koller D, Pfeffer A. Probabilistic frame-based systems. In: Proceedings of 15th national conference on artificial intelligence (AAAI). Madison (Wisconsin); 1998.
[34] König J, Nordstrom L, Ekstedt M. Probabilistic relational models for assessment of reliability of active distribution management systems. In: Proceedings of 11th IEEE international conference on probabilistic methods applied to power systems (PMAPS); 2010. p. 454–9.
[35] Lai C-D, Xie M. Stochastic ageing and dependence for reliability. New York: Springer; 2007.
[36] Langseth H. Bayesian networks in reliability: the good, the bad and the ugly. Advances in mathematical modeling for reliability. Amsterdam (Netherland): IOS Press; 2008.
[37] Langseth H, Portinale L. Bayesian networks in reliability. Reliability Engineering and System Safety 2007;92(1):92–108.
[38] Léger A, Duval C, Farret R, Weber P, Levrat E, Iung B. Modeling of human and organizational impacts for system risk analyses. In: Proceedings of 9th international probabilistic safety assessment and management conference. Hong Kong (China); 2008.
[39] Léger A, Weber P, Levrat E, Duval C, Farret R, Iung B. Methodological developments for probabilistic risk analyses of socio-technical systems. Journal of Risk and Reliability 2009;223(4):313–32.

[40] Léger JB, Iung B, Beca AFD, Pinoteau J. An innovative approach for new distributed maintenance system: application to hydro power plants of the REMAFEX project. Computers in Industry 1999;38(2):131–48.
[42] Lin D, Zuo M, Yam R. General Sequential Imperfect preventive maintenance models. International Journal of Reliability, Quality and Safety Engineering 2000;7(3):253–66.
[43] Mahadevan S, Zhang R, Smith N. Bayesian networks for system reliability reassessment. Structural Safety 2001;23(3):231–51.
[44] Marseguerra M, Zio E. Condition-based maintenance optimization by means of genetic algorithms and Monte Carlo Simulation. Reliability Engineering and System Safety 2002;77:151–66.
[45] Mayer F, Morel G, Iung B, Léger J-B. Integrated manufacturing system meta-modelling at the shop-floor level. In: Proceedings of the advanced summer institute conference. Toulouse (France): Lab. for Automation and Robotics of Patras—Greece; 1996. p. 257–64.
[46] Medina-Oliva G, Weber P, Simon C, Iung B. Bayesian networks applications on dependability, risk analysis and maintenance. In: Proceedings of 2nd IFAC workshop on dependable control of discrete system, DCDS'09. Bari (Italy); 2009.
[47] Medina-Oliva G, Weber P, Levrat E, Iung B. Use of probabilistic relational model (PRM) for dependability analysis of complex systems. In: Proceedings of 12th LSS IFAC symposium large scale systems, Villeneuve d'Ascq (France); 2010.
[48] MIMOSA. Machine information management open system alliances; 2009. ⟨www.mimosa.org⟩.
[49] Mohaghegh Z. On the theoretical foundations and principles of organizational safety risk analysis. Doctor of Philosophy of the Faculty of the Graduate School of the University of Maryland; 2007.
[50] Muller A, Suhner M-C, Iung B. Formalisation of a new prognosis model for supporting proactive maintenance implementation on industrial system. Reliability Engineering and System Safety 2008;93(2):234–53.
[51] Øien. A framework for the establishment of organisational risk indicators. Reliability engineering & systems safety 2001;74(2):147–67.
[52] Papazoglou IA, Bellamy LJ, Hale AR, Aneziris ON, Ale BJM, Post JG, Oh JIH. I-risk development of an integrated technical and management risk methodology for chemical installations. Journal of Loss Prevention in the Process Industries 2003;16:575–91.
[53] Parida A. Development of a multi-criteria hierarchical framework for maintenance performance measurement. Doctoral thesis. Division of operation and maintenance engineering. Luleå; University of Technology; 2006.
[54] Pearl J. Probabilistic reasoning in intelligent systems: networks of plausible inference. San Francisco (USA): Morgan Kaufmann Publishers Inc.; 1988.
[55] Pfeffer A, Koller D, Milch B, Takusagawa KT. SPOOK: a system for probabilistic object-oriented knowledge representation. In: Proceedings of the 14th annual conference on uncertainty in AI (UAI). Stockholm (Sweden); 1999.
[56] Pfeffer AJ. Probabilistic reasoning for complex systems. PhD thesis. Stanford University; 2000.
[57] Pham H, Wang H. Imperfect maintenance. European Journal of Operational Research 1996;94(3):425–38.
[58] Pollino CA, Woodberry O, Nicholson A, Korb K, Hart BT. Parameterisation and evaluation of a Bayesian network for use in an ecological risk assessment. Environmental Modelling & Software 2007;22(8):1140–52.
[59] Sargent RG. Verification and validation of simulation models. In: Proceedings of 1998 winter simulation conference; 1998. p. 121–30.
[60] Schönbeck M, Rausand M, Rouvroye J. Human and organisational factors in the operational phase of safety instrumented systems: a new approach. Safety Science 2010;48:310–8.
[61] Simon C, Weber P. Evidential networks for reliability analysis and performance evaluation of systems with imprecise knowledge. IEEE Transactions on Reliability 2009;58(1):69–87.
[63] SKOOB. Structuring knowledge with object oriented Bayesian nets (SKOOB) project. Ref. ANR PROJET 07 TLOG 021; 2011 ⟨http://skoob.lip6.fr⟩.
[64] Sommestad T, Ekstedt M, Johnson P. A probabilistic relational model for security risk analysis. Computers & Security, 2010;29(6):659–79.
[65] Takata S, Kimura F, van Houten FJAM, Westkämper E, Shpitalni M, Ceglarek D, Lee. J. Maintenance: changing role in life cycle management. Annals of CIRP 2005;53(2):643–55.
[66] Torres Toledano JG, Succar LES. Bayesian networks for reliability analysis of complex systems. Lecture Notes in Artificial Intelligence 1998;1484:195–206.
[67] Torti L, Wuillemin P-H, Gonzales C. Reinforcing the object-oriented aspect of probabilistic relational models.in: Proceedings of Probabilistic Graphical Models; 2010. p. 273–80.
[68] Trucco P, Cagno E, Ruggeri F, Grande O. A Bayesian belief network modelling of organisational factors en risk analysis: a case study in maritime transportation. Reliability Engineering and System Safety 2008;93(6):845–56.
[69] Utkin L, Coolen F. New metaheuristics, neural & fuzzy techniques in reliability, Series: computational intelligence in reliability engineering. In: Levitin G, editor. Imprecise reliability: an introductory overview, vol. 2;2007. p. 261–306 [Chapter 10].
[70] Valdez-Flores C, Feldman RM. A survey of preventive maintenance models for stochastically deteriorating single-unit systems. Naval Research Logistics 1989;36:419–46.
[71] Van Noortwijk JM. A survey of the application of gamma processes in maintenance. Reliability Engineering and System Safety 2009;94(1):2–21.
[72] Von Bertalanffy L. General system theory: foundations, development, applications. New York: George Braziller Inc.; 1976.
[73] Wang H. A survey of maintenance policies of deteriorating systems. European Journal of Operational Research 2002;139(3):469–89.
[74] Weber P, Theilliol D, Aubrun C. Component reliability in fault-diagnosis decision making based on dynamic Bayesian networks. Journal of Risk and Reliability in the Proceedings of the Institution of Mechanical Engineers, Part O 2008;222(2):161–72.
[75] Weber P, Jouffe L. Complex system reliability modeling with Dynamic Object Oriented Bayesian Networks (DOOBN). Reliability Engineering and System Safety 2006;91(2):149–62.
[76] Weber P, Medina-Oliva G, Simon C, Iung B. Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. Engineering Applications of Artificial Intelligence 2012;25(4):671–82, http://dx.doi.org/10.1016/j.engappai.2010.06.002.
[77] Weber P, Suhner M-C. An application of Bayesian networks to the performance analysis of a process. In: Proceedings of European conference on system dependability and safety (ESRA 2002/lambda-Mu13). Lyon (France); 2002.
[78] Weber P, Suhner M-C, Iung B. System approach-based Bayesian network to aid maintenance of manufacturing process. In: Proceedings of 6th IFAC symposium on cost oriented automation, low cost automation; 2001.
[79] Zhang N, Poole D. Exploiting causal independence in Bayesian network inference. Journal of Artificial Intelligence Research 1996;5:301–28.

Engineering Applications of Artificial Intelligence 25 (2012) 671–682

Contents lists available at ScienceDirect

Engineering Applications of Artificial Intelligence

journal homepage: www.elsevier.com/locate/engappai

Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas

P. Weber*, G. Medina-Oliva, C. Simon, B. Iung

CRAN-Nancy-Université-CNRS, UMR7039, Boulevard des Aiguillettes, B.P. 70239, F-54506 Vandœuvre lès Nancy, France

ARTICLE INFO

Article history:
Received 21 December 2009
Received in revised form
13 May 2010
Accepted 1 June 2010
Available online 16 July 2010

Keywords:
Bayesian networks
Dependability
Risk analysis
Maintenance
Reliability
Safety

ABSTRACT

In this paper, a bibliographical review over the last decade is presented on the application of Bayesian networks to dependability, risk analysis and maintenance. It is shown an increasing trend of the literature related to these domains. This trend is due to the benefits that Bayesian networks provide in contrast with other classical methods of dependability analysis such as Markov Chains, Fault Trees and Petri Nets. Some of these benefits are the capability to model complex systems, to make predictions as well as diagnostics, to compute exactly the occurrence probability of an event, to update the calculations according to evidences, to represent multi-modal variables and to help modeling user-friendly by a graphical and compact approach. This review is based on an extraction of 200 specific references in dependability, risk analysis and maintenance applications among a database with 7000 Bayesian network references. The most representatives are presented, then discussed and some perspectives of work are provided.

1. Introduction and problem statement

The management of complex industrial systems contributes to higher competitiveness and higher performances at lower costs. In that way, the relevance of the maintenance and dependability analyses increased due to their role in improving availability, performance efficiency, products quality, on-time delivery, environment and safety requirements, and total plant cost effectiveness at high levels (Alsyouf, 2007; Kutucuoglu et al., 2001). Nowadays, one of the major problems in the dependability field is addressing the system modeling in relation to the increasing of its complexity. This modeling task underlines issues concerning the quantification of the model parameters and the representation, propagation and quantification of the uncertainty in the system behavior (Zio, 2009).

In previous years, the reliability and risk analysis of systems were studied by making assumptions simplifying the study. One of these assumptions is to focus the study only on the technical part of the system. This assumption is no longer valid, since it has been shown the importance of organizational and human factors contributions (Leveson et al., 2009). Indeed, if studies were centered on technical aspects of systems until seventies (Villemeur, 1992), several major accidents, such as the Three Miles Island nuclear accident and the Bhopal catastrophe have pointed out cause operator errors and organizational malfunctions. These accidents allowed the scientific community to present and develop, in eighties, first methods centered on the analysis of these human errors. It led to the expansion of the human reliability analysis (HRA). But other accidents (Challenger explosion, Chernobyl nuclear accident …) have emphasized, in nineties, the importance of organizational malfunctions in their occurrences and, have contributed to the emergence of different theories for the study of these organizational issues: normal accident (Perrow, 1990; Weick, 2001) and high reliability organizations (Robert, 1990; Léger et al., 2008, 2009).

As a consequence, innovative studies aim at covering the whole of these causes (technical, human and organizational). Nevertheless, such analyses are often difficult to achieve because they require a lot of resources. This matter adds complexity to the systems' modeling due to the interaction between different technical, human, organizational and nowadays environmental factors which are necessary to quantify failure scenarios and risky situations. Thus, the challenge is to formalize a model of a complex system integrating all these aspects (Trucco et al., 2008; Kim et al., 2006) (Fig. 1).

Furthermore, while modeling these factors, it is required to take into account the knowledge integration of diverse natures such as qualitative and quantitative with several abstraction levels. The organization and human analyses are more naturally modeled with a qualitative knowledge (to describe situations,

* Corresponding author.
E-mail addresses: philippe.weber@cran.uhp-nancy.fr (P. Weber), gabriela.medina-oliva@cran.uhp-nancy.fr (G. Medina-Oliva), christophe.simon@cran.uhp-nancy.fr (C. Simon), benoit.iung@cran.uhp-nancy.fr (B. Iung).

0952-1976/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.engappai.2010.06.002

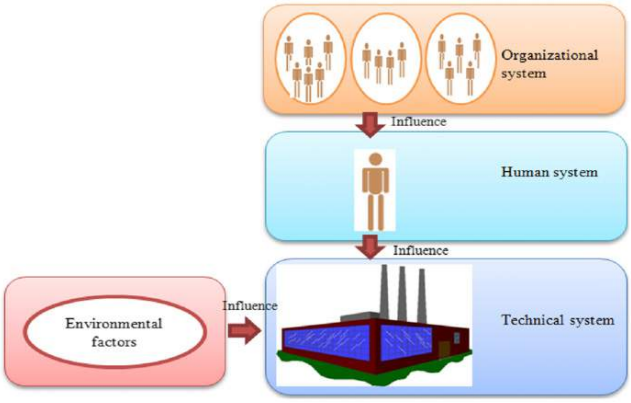


Fig. 1. Context of the complex system to be modeled.

scenarios…) such as knowledge represented in failure mode, effects, and criticality analysis (FMECA), HAZard OPerability (HAZOP), probabilistic risk assessment (PRA) analysis, etc.; and in other hand, the technical level is usually known with quantitative information (failure rates, unavailability level, Mean Time To Failure (MTTF), etc.) (Røed et al., 2008).

A complementary point of view to be modeled for the system is the temporal dimension (system dynamics) which consists in describing phenomenon such as: sequences in scenarios, degradations of components, evolution of symptoms corresponding to deterioration mechanisms, impact of preventive maintenance actions on the degradation, influence of environmental conditions and effects of the operation conditions on the evolution of the component states.

Once assessed the failure probability and risk associated to a system situation, the information is provided to support the decision making process. It implies to quantify the uncertainty and imprecision on parameters, for example, the uncertainty of the failure occurrence and its consequences (Zio, 2009).

Therefore, the main characteristics to be modeled in a system for assessing dependability and maintenance aspects are:

- the complexity and size of the system (large-scale systems) (Zio, 2009),
- the temporal aspects (Labeau et al., 2000),
- the integration of qualitative information with quantitative knowledge on different abstraction levels (Papazoglou et al., 2003; Delmotte, 2003),
- the nature of multi-state components (Griffith, 1980),
- the dependences between events such as failures (Torres-Toledano and Sucar, 1998),
- uncertainties on the parameter estimation (Zio, 2009).

For modeling these requirements, there are some classical dependability methods such as fault trees, Markov chains, dynamic fault trees, Petri nets and Bayesian networks (BN). In the recent literature, it is observed a growing interest focused on BN. This modeling method is not the solution to all problems, but it seems to be very relevant in the context of complex systems (Langseth, 2008).

Indeed some papers such as Mahadevan et al. (2001), Boudali and Dugan (2005b), Langseth and Portinale (2007) and Langseth (2008) show the increasing interest on the use of BN to estimate and to improve reliability and safety of systems over the last decade. For example, during the period 1999–2009, RESS journal (Reliability Engineering and System Safety), well known in dependability area, shows an increment of 100% of a ratio consisting on the paper number dedicated to the application of BN to reliability (or risk) divided by the total amount of papers. This type of ratio has strengthened our interest to analyze the evolution of the literature about BN and their applications on dependability, risk analysis and maintenance. For this purpose, we have built a database of references from 1990 to 2008 with different bibliographical research tools (i.e. google scholar, Sciencedirect, Web of Knowledge …). In this paper, the most relevant articles according to their citation number were referenced until 2008. Nonetheless, some citations on "hot topics" of research until 2009 are also given.

The rest of this paper is organized as follow. Section 2 is introducing the bases of BN and explaining why they are suitable to model complex systems. Section 3 shows a bibliographical review of the relevant research directions for modeling dependability, risk analysis and maintenance problems with BN. Section 4 presents a comparison of the BN modeling capabilities with other modeling methods such as Fault Tree, Markov Chains and Petri Nets. Finally, the conclusions are given by integrating also highlights future research directions.

2. BN in general

BN appear to be a solution to model complex systems because they perform the factorization of variables joint distribution based on the conditional dependencies. The main objective of BN is to compute the distribution probabilities in a set of variables according to the observation of some variables and the prior knowledge of the others. The principles of this modeling tool are explained in Jensen (1996) and Pearl (1988).

2.1. Recall of BN characteristics

A BN is a directed acyclic graph (DAG) in which the nodes represent the system variables and the arcs symbolize the dependencies or the cause–effect relationships among the variables. A BN is defined by a set of nodes and a set of directed arcs. A probability is associated to each state of the node. This probability is defined, *a priori* for a root node and computed by inference for the others.

The computation is based on the probabilities of the parent's states and the conditional probability table (CPT). For instance, let us consider two nodes A and B; with two states (S_{*1} and S_{*2}) each; structuring the BN (Fig. 2). The *a priori* probabilities of node A are defined as in Table 1.

A CPT is associated to node B. This CPT defines the conditional probabilities $P(B|A)$ attached to node B with a parent A, to define the probability distributions over the states of B given the states of A.

This CPT is defined by the probability of each state of B given the state of A (Table 2).

Thus, the BN inference computes the marginal distribution $P(B=S_{B1})$:

$$P(B=S_{B1})=P(B=S_{B1}|A=S_{A1}).P(A=S_{A1})+P(B=S_{B1}|A=S_{A2}).P(A=S_{A2}) \quad (1)$$

The added value of a BN is linked to the computation of the probabilities attached to a node state, given the state of one or

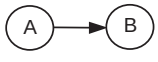


Fig. 2. Basic example of a BN.

Table 1
A Priori probabilities of the node A.

A	
S_{A1}	$P(A=S_{A1})$
S_{A2}	$P(A=S_{A2})$

Table 2
CPT of the node B given the node A.

A	S_{A1}	S_{A2}	
B	S_{B1}	$P(B=S_{B1}\|A=S_{A1})$	$P(B=S_{B1}\|A=S_{A2})$
	S_{B2}	$P(B=S_{B2}\|A=S_{A1})$	$P(B=S_{B2}\|A=S_{A2})$

several variables. BN is a powerful modeling tool for complex systems because providing a lot of modeling advantages.

Indeed for providing global reliability estimation, BN permit to merge knowledge of diverse natures in one model: data from feedback experience, experts' judgment (express through logical rules, equations or subjective probabilities), the behavior of the studied system (functional and dysfunctional analysis) and observations. Moreover to study and to analyze complex systems, it is necessary to model the interaction between organizational, human and technical factors. BN establishes cause–effect relationships between these factors for modeling their interactions. For example, BN can model the effect of maintenance actions and barriers' impact on the global system risk analysis (Léger et al. (2009)). Usually, it is necessary to use several sources of information for developing a model. However, there is few feedback data particularly in the domains of dependability, risk analysis and maintenance. For this reason, the research works use mainly the experts' judgment to build the structure of models (Celeux et al., 2006).

A general inference mechanism (that permits the propagation as well as the diagnostic) is used to collect and to incorporate the new information (evidences) gathered in a study. The Bayes' theorem is the heart of this mechanism and allows updating a set of events' probabilities according to the observed facts and the BN structure. It makes the strength of this knowledge management tool.

3. Literature on BN application to dependability, risk analysis and maintenance

In the specialized literature about BN, most of the references are related to the learning and inference algorithms. Nonetheless, we found a set of 200 articles about the application of BN to dependability, risk analysis and maintenance. It shows a continuous increment of the number of references and, a scientific and industrial interest for this tool. Most of the selected references are about dependability with 61% of the publications, risk analysis with 26% and maintenance with 13% (Fig. 3).

3.1. Application to dependability

The dependability aim is to provide a prediction of a parameter (remaining time to fail, MTTF, reliability, etc.) which is an input data for the decision step (for example maintenance optimization, dependable system design …). Thus, it is necessary to take into account some aspects such as multi-state elements (Griffith, 1980), failures' dependencies (Lai and Xie, 2006), system redundancy (Tavakkoli-Moghaddam et al., 2008), dynamic evolution (e.g. the degradation process) (Lai and Xie, 2006) and to incorporate the influencing factors of a system dependability such as operations conditions (Bazovsky, 1961).

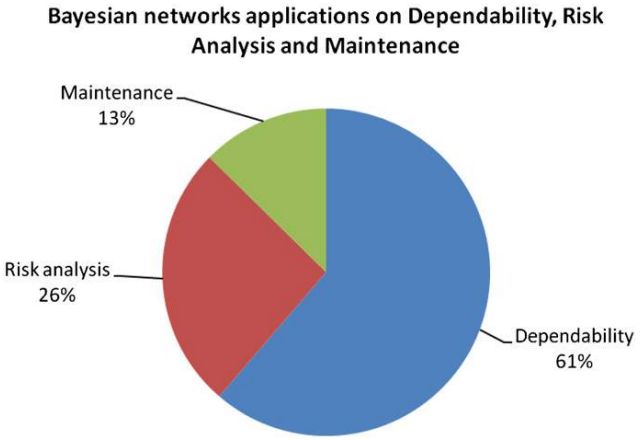


Fig. 3. Distribution of references on the topics.

BN models are more and more used in dependability analyses to support aspects such as reliability, availability and maintainability. Fig. 4 shows the number of references per year related to the BN application to dependability analyses. Since 2000, it is observed a significant rising of 800% on their application due to the modeling benefits that BN can offer. Fig. 5 shows the main topics evolution of BN literature and its application on this field with some relevant references.

The first major contributions have been done by Castillo et al. (1997), Torres-Toledano and Sucar (1998), Arroyo et al. (1998) and Kang and Golay (1999). The original work' objectives handled by Torres-Toledano and Sucar (1998) and Arroyo et al. (1998) were: (a) to estimate a system reliability including possibilities of failures' dependencies; (b) to model complex systems (2003).

At the same time, BOLARR project emphasizes dynamic modeling for risk analyses (Welch and Thelen, 2000) through BN. Simultaneously, the SERENE project aims at formalizing the experts' reasoning in order to evaluate the different aspects of dependability on critical systems (Bouissou et al., 1999). As one of its objective was to provide a model with several abstraction levels, this project is also based on building a hierarchical object oriented BN in order to incorporate the influence factors of the system dependability.

With reference to software reliability area, there are some significant works whose goal is to assess a reliability prediction within software taking into account the operational conditions (Bai, 2005; Bai et al., 2005). In the context of a software safety standard, Axel and Helminen (2001) present how a BN can be merged with a BN on the reliability estimation of software based on digital systems. Helminen and Pulkkinen (2003) exploit the BN abilities when combining experts' judgments and the feedback experience data to estimate the reliability of a motor protection critical system. Wilson and Huzurbazar (2006) describe different application contexts of BN in the reliability field: known or unknown conditional probabilities, taking into account new data in order to improve the conditional probabilities estimation.

After this first step focused on static BN, the community focused also in dynamic models. Welch and Thelen (2000) worked on the comparison between Markov Chains and BN application to the reliability evaluation. More recent studies have focused on the reliability estimation including the temporal aspect by the use of dynamic Bayesian networks (DBN). Boudali and Dugan (2005a,b) and Montani et al. (2006) proposed the integration of the dynamic aspect by the transformation of dynamic fault trees (DFT) into DBN. Montani et al. (2006) develop a tool to translate DFT based

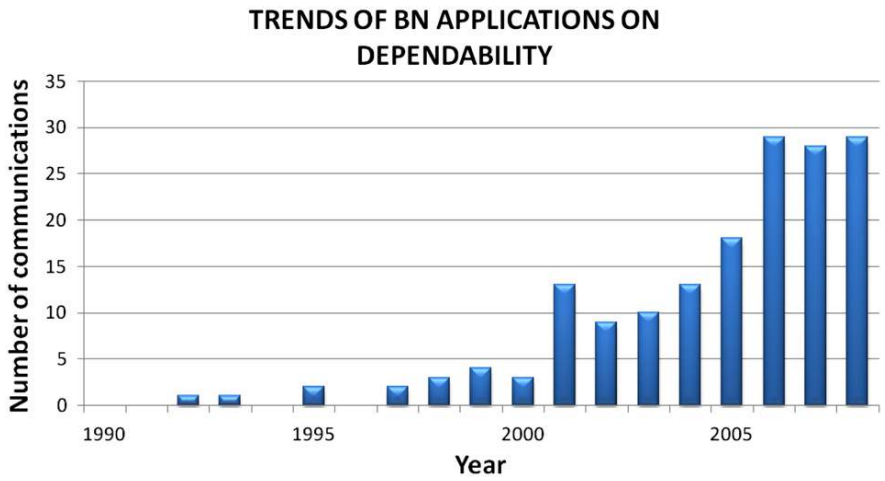


Fig. 4. Publication number related to Bayesian Network application on dependability.

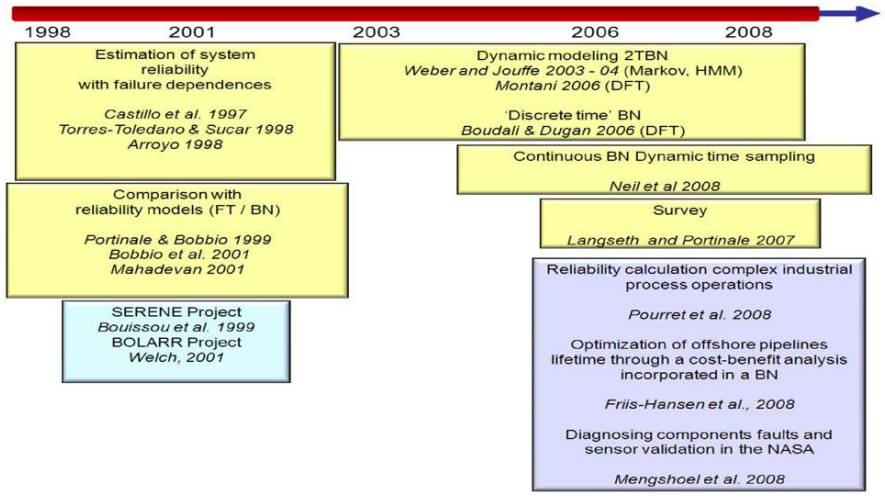


Fig. 5. Most relevant papers of BN application on dependability field.

on two time slices BN (2TBN). Portinale et al. (2010) present the software called RADYBAN (Reliability Analysis with DYnamic BAyesian Networks) which supports an approach to reliability modeling and analysis based on the automatic translation from DFT into a DBN.

In Weber and Jouffe (2006), the model is based on dynamic object oriented BN (DOOBN) and the model structure is deduced from the functional analysis (knowledge represented by SADT method) and malfunctioning (knowledge formalized by FMECA). DBN models are able to represent the impacts of the operational conditions (e.g. maintenance actions, production levels, environmental conditions…) on system reliability by means of exogenous variables (Weber et al., 2004).

One of the current limitations of BN is that they can only deal with discrete variables. Nonetheless, in the reliability field there are some phenomena which should be taken into account with continuous nature (i.e. operating and environmental variables). For that reason, one of the important topics of research is the development of inference algorithms for hybrid BN. These models contain discrete and continuous variables. In that sense, Boudali and Dugan (2006) propose to use continuous nodes with sampling of time to model the failure distribution of the components in a reliability model. In the same way, Neil et al. (2008, 2009) built hybrid BN including discrete and continuous nodes to estimate the system reliability. The algorithm combines a dynamic time sampling to the classical propagation algorithms. The time sampling of the continuous variables is updated by taking into account the evidences. The authors present this concept as an alternative method to simulation methods such as Markov Chain Monte Carlo (MCMC).

Langseth et al. (2009) propose a synthesis about the inferences in hybrid BN in the context of reliability analysis. They explore four approaches of inference in hybrid BN: discretization, Mixtures of Truncated Exponentials (MTE), variational methods and Markov Chain Monte Carlo (MCMC). They are interested in obtaining approximations of low probability events in the tails of approximations. For that purpose, the best suited appears to be the MTE framework because it balances the need for good approximations in the tail of the distributions with not-too-high computational complexity.

In addition, Langseth & Portinale (2007) wrote a synthesis about different building steps in a BN and the use of this formalism in reliability. Some applications of BN exist in this area, for example the diagnosis of components faults and sensor validation in the NASA (Mengshoel et al., 2008), the reliability calculation in complex industrial process operations such as the

industry of pulp and paper (Pourret et al., 2008) and the optimization of a strategic decision for improving the offshore pipelines lifetime through a cost-benefit analysis (Friis-Hansen and Hansen, 2008).

Complementary contribution is presented by Doguc and Ramirez-Marquez (2009) who introduce a holistic method for estimating system reliability by automatically constructing a BN from historical data on the system. In essence, the method replaces the need of an expert to find associations among the components with the raw data related to the component and system behavior. The proposed method automates the process of BN construction by feeding raw system behavior data to the K2 algorithm (a commonly used association rule mining algorithm).

Finally, an interesting problem is tackled by Simon et al. (2008) and concerns how BN can handle epistemic and random uncertainties. By extending the usual state of affairs in probability theory and the corresponding belief measure assignment to Dempster-Shafer structures, the authors extended BN to evidential networks based on an extended Bayesian inference. Evidential networks can deal with interval valued probabilities (Simon et al., 2008), fuzzy valued probabilities (Simon and Weber, 2009a) and multi-states systems for reliability and performance evaluation (Simon and Weber, 2009b).

So far, Table 3 presents a synthesis of the modeling aspects in dependability area that have been covered by research works, those about which researchers are still working on and, those which are still under-developed.

3.2. Applications in risk analysis

Risk analysis is a technique for identifying, characterizing, quantifying and evaluating critical event occurrence. The quantification of risk includes the estimation of the likelihood (e.g., frequencies) and the consequences of hazard occurrence. The estimation of the likelihood of hazard occurrence depends greatly on the reliability of the system's components, the interaction of the components taking the system as a whole and human–system interactions. Risk evaluation needs a systematic research of accidental scenarios, including failure rates for the component (e.g. safety barriers) as well as for operator behavior (human factor) within an evolving environment. Additionally, in these kinds of analyses, low probability events and the dependencies between variables must be taken into account. The objective of these analyses is to provide the elements that help decision making in terms of design evolution, operation, preparation and risk management (Modarres et al., 1999).

Since 2001, BN have been used to analyze risky situations. Particularly, BN represent a useful formalism in the risk analyses domain due to their ability to model probabilistic data with dependencies between events. Fig. 6 shows the development of BN scientific literature focused on risk analysis. From 2001 to 2008, the number of references per year increased by 4.

Fig. 7 shows the main steps of the evolution of BN literature and its application in risk analysis based on the most relevant papers. The first contributions were made by Hudson et al. (2002).

Table 3
Overview of the modeling aspects in dependability area.

Dependability items	Main contributions	Theoretical contribution	Methodological contribution	Applicative contribution
Covered aspects				
Considering multi-state elements.	Torres-Toledano and Sucar, (1998)		×	
	Arroyo et al. (1998)			×
	Kang and Golay (1999)			×
	Helminen and Pulkkinen (2003)	×		×
Considering dependencies between events.	Boudali and Dugan (2005b)		×	
	Bouissou et al. (1999)		×	
	Wilson and Huzurbazar (2006)		×	
Aspects which researchers are still working on				
Including the temporal aspect in reliability analyses.	Boudali and Dugan (2005 a,b)		×	
	Montani et al. (2006)		×	
	Neil et al. (2008)		×	
	Welch and Thelen (2000)		×	
	Portinale et al. (2010)		×	
Considering exogenous variables such as environmental conditions to optimize maintenance decisions	Weber et al. (2004)		×	
	Ben Salem et al. (2006)		×	
	Friis-Hansen and Hansen (2008)			×
	Bai (2005)		×	
Including continuous variables in the dependability analysis	Boudali and Dugan (2006)	×		
	Neil et al. (2009)	×		
	Langseth et al. (2009)	×		
Characterizing, representing and propagating uncertainties (epistemic; random and numeric) in reliability analysis of complex systems	Simon and Weber (2008, 2009a, b)		×	
Constructing an automated BN model without human expertise	Doguc and Ramirez-Marquez (2009)		×	
Managing models with great number of variables	SKOOB Project 2008			×
Under-developed aspects (with minor results)				
Integrating, in one model, the technical, organizational, informational, decisional and human aspects and the impacts on the system's functioning.				

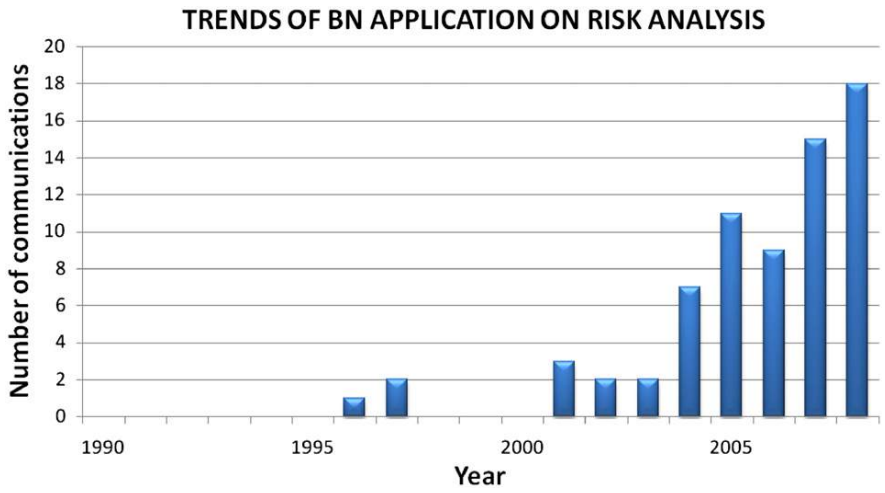


Fig. 6. Publication number related to Bayesian Network applications on risk analysis.

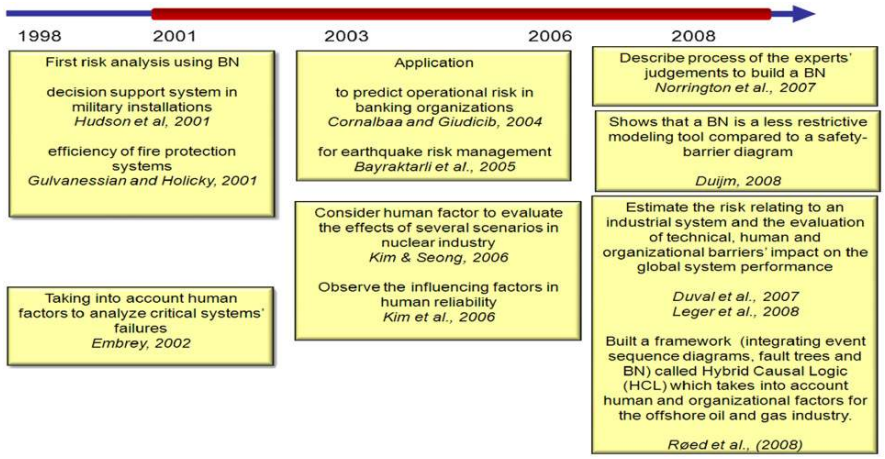


Fig. 7. Most relevant papers of BN application on risk analysis.

The authors use BN as a key element of a decision support system for assessing terrorist threats against military installations. At the same period, Gulvanessian and Holicky (2001) proposed a BN to analyze the efficiency of fire protection systems and to find the most effective arrangements in real situations.

Øien (2001) proposed a framework to integrate organizational risk indicators for assessing the risk impact. This model could be used to identify qualitatively the root causes of accidents or incidents. The objective is to develop a model for risk control purposes so the organizational risk indicators should be acquired with a certain frequency. For the model quantification, the author used BN due to the possibility of multi-state representation and the intuitive representation of causal relationships linking the organizational factors to the quantitative risk model.

Embrey (2002) takes into account human factors by using influence diagrams to analyze and to anticipate critical systems' failure. Also, Kim and Seong (2006) describe a BN model including human factors to evaluate the effects of several scenarios in the nuclear industry. The same authors use BN to observe the influence factors in human reliability (Kim et al., 2006).

Complementary contributions were made by Cornalba and Giudici (2004) who develop a work in which a BN approach is used to develop a statistical model to measure and, consequently, to predict the operational risks to which a banking organization is subjected to. Bayraktarli et al. (2005) worked with the application of BN to earthquake risk management. The authors propose that the uncertainties associated with all elements in the functional chain of an earthquake (from the source mechanism, site effects, structural response, damage assessments and consequence assessment) can be handled consistently using a BN. Straub (2005) demonstrates the advantages of BN for the application in risk assessments for natural hazards. Lee and Lee (2006) propose a quantitative assessment framework integrating the inference process of BN to the traditional probabilistic risk analysis in order to consider the effects predicted from an evolution of the environmental conditions of waste disposal facilities.

In the maritime field, BN approaches are applied to consider the human and organizational factors in a risk analysis. Norrington et al. (2007) describe elicitation process of the experts' judgments to build a BN. A significant BN approach was developed by Trucco et al. (2008) to model the Maritime Transportation System by taking into account its different actors (i.e., ship-owner, shipyard, port and regulator) and their mutual influences. The model is used in a case study for the quantification of Human and Organizational Factors in the risk analysis carried out at the preliminary design stage of high speed craft.

Røed et al. (2008) built a framework taking into account human and organizational factors within a framework called hybrid causal logic (HCL). This framework let BN be logically and probabilistically integrated into event sequence diagrams and fault trees in order to

Table 4
Overview of the modeling aspects in risk analysis area.

Items	Main contributions	Theoretical contribution	Methodological contribution	Applicative contribution
Covered aspects				
Modeling the dependencies between events	Hudson et al. (2002)			×
	Gulvanessian and Holicky (2001)		×	
	Lee and Lee (2006)			×
	Straub (2005)			×
	Bayraktarli et al. (2005)			
	Cornalba and Giudici (2004)			
Quantitatively estimating the risk with barriers' impact on the system	Léger et al., 2008		×	
	Léger et al. (2009)		×	
Aspects which researchers are still working on				
Integrating the technical, human and organizational aspects with different abstraction levels	Øien (2001)		×	
	Kim et al. (2006)			×
	Trucco et al. (2008)			×
	Røed et al. (2008)			×
	Norrington et al. (2007)			×
Integrating qualitative information (functional, organizational analysis) with quantitative knowledge (technical and financial levels)	Léger et al., 2008		×	
	Léger et al. (2009)		×	
	Røed et al. (2008)			×
Managing models with great number of variables	SKOOB project 2008			×
Under-developed aspects (with not significant results)				
Taking into account the resilient aspect of human operators and organizations.				
Including the temporal aspect in the risk analysis				
Characterizing, representing and propagating uncertainties (epistemic; random and numeric) in risk analysis				
Constructing an automated BN model without human expertise				

perform a risk analysis. Then, this framework is applied to the offshore oil and gas industry. A recent comparison between BN and standard modeling methods is made by Duijm (2009) showing that BN is a less restrictive modeling tool compared to a safety-barrier diagram. For example, a comparison is made between the number of states that can be modeled with a barrier diagram (Boolean model) and a BN (multi-state representation). In risk analyses, the recent publications of Léger et al. (2009) propose a BN modeling by structuring the model in different levels: organization/actions/technique. The aim of these works is to quantitatively estimate the risk related to an industrial system operation (occurrence probability of scenarios) and the evaluation of technical, human and organizational barriers' impact on the global system performance. The originality of these models is the BN-based unification formalism of functional, dysfunctional, behavioral and organizational knowledge of a system.

The use of BN is developing rapidly mainly due to its capability to represent complex systems with dependencies between variables. Particularly, for risk analyses, BN are well adapted due to its capability to quantify low probability events. In that sense, Hanea and Ale (2009) work on an overall model which takes into account people, fire fighters' action, structure of the building and characteristics of the building and, the environment in order to analyze low-probability-high-consequence scenarios of human fatality risk in building fires. In addition, Cheon et al. (2009) worked about the prediction of daily ozone states in Seoul, Korea. They combine real measured data and expert knowledge to overcome the complexity of O_3 reactions.

So far, Table 4 presents a synthesis of the modeling aspects in risk analyses area that have been covered by research works, those about which researchers are still working on and, those which are still under-developed.

3.3. Application in maintenance

For developing an appropriate maintenance concept, maintenance must be considered holistically. In that way, factors that technically describe each system to be maintained (e.g., functional and dysfunctional analyses, causal relationships between degradations, etc.), as well as factors that describe the interrelations between the different systems (e.g. maintenance actions) and, factors that describe the general organizational structure, should be addressed. If some aspects are not considered (e.g. due to inaccurate analysis or loss of data or knowledge), the maintenance concept will never reach its full potential (Waeyenbergh and Pintelon, 2004). The critical areas for assessing maintenance performances vary from company to company but, generally include areas such as financial or cost-related issues, health and safety and environment related issues, processes-related issues, maintenance task related issues and learning growth and innovation related issues, while at the same time comprising the internal and external aspects of the company (Parida, 2006).

BN are used in works concerning maintenance decisions and performance evaluation as illustrated Fig. 8. In 1999, a threefold increase in the beginning of research activities can be between 2000 and 2008. The activities in this field are recent so, it exists in few references. In Fig. 9, the most relevant literature on BN for application in maintenance is summarized.

Kang and Golay (1999) proposed a model with influence diagrams which consider evidences. The purpose is to estimate the future state of a system after a particular action. The proposal of an action is made based on the conditional probabilities and the utility values.

The performances' analyses of a system and the establishment of the prognostic process model are the key points for maintenance optimization. The BN model developed by Weber et al.

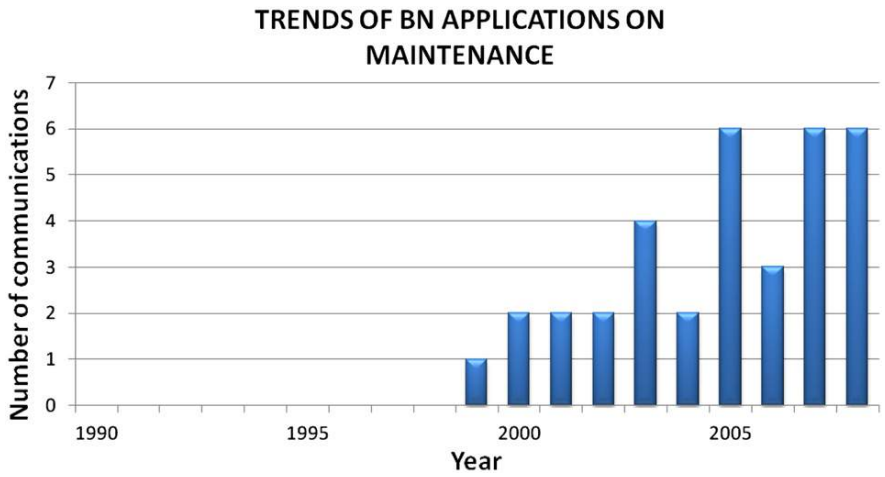


Fig. 8. Publication number related to Bayesian Network application on maintenance.

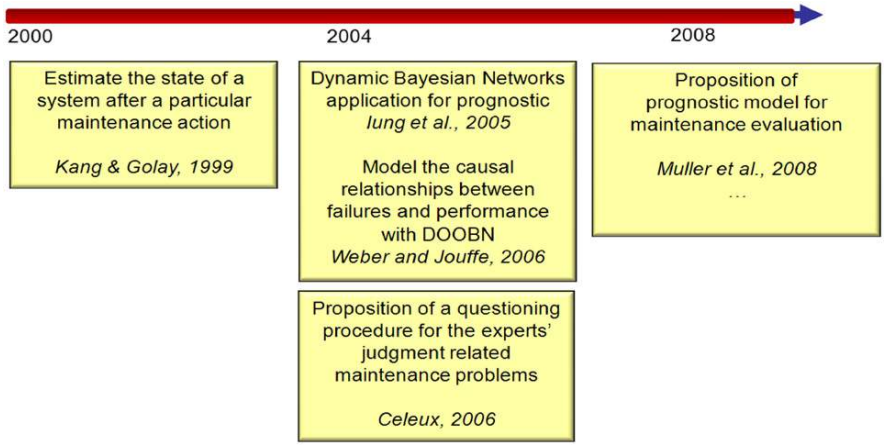


Fig. 9. Most relevant papers of BN application on maintenance.

(2001) is built including the functional and dysfunctional analysis of the system. It allows its global performance estimation (Muller et al., in press).

Weber and Jouffe (2006), Iung et al. (2005) and Borgia et al. (2009) investigate the use of DBN for modeling the causal relationships between degradation/cause/consequence. Moreover, utility nodes are integrated into the probabilistic model.

For modeling a real maintenance problem, Celeux et al. (2006) propose a questioning procedure dedicated to the elicitation of experts' judgment. This procedure is set up by rules to collect information and to build the network structure. The model's parameters are determined by feedback data and later by expertise.

Recently, De Melo and Sanchez (2008) have worked on the prediction of delays for software maintenance projects. In this approach, they considered the factors that could induce uncertainty during the maintenance process such as the maintenance complexity, the expertise of professionals, the system documentation, the opportunity of using new resources, etc. This study helps to compute the probability distribution of a maintenance project delay based on project features.

So far, Table 5 presents a synthesis of the modeling aspects in maintenance area that have been covered by research works, those about which researchers are still working on and, those which are still under-developed.

4. Bayesian networks modeling capabilities

This section corresponds to the bibliography related to the comparison of the modeling capabilities between BN and three classical methods of dependability evaluation: Fault Trees (FT), Markov Chains (MC) and Petri Nets (PN). Some publications are also mentioned with regards to the transformation (translation) of the previous methods into a BN.

4.1. Fault trees (FT)

Fault Trees are based on the hypothesis of Boolean representation of elementary events. The computing of probability in fault trees is efficiently solved by binary decision diagrams (BDD) which enable an exact computation, considering dependencies between the branches due to redundancy of elementary events unfactorized. However, it is necessary to respect the hypothesis of elementary events independence (IEC61025, 2006).

In relation to the problem statement developed in this paper, FT is a very interesting modeling solution since it allows to consider dependencies between events and to integrate different kinds of knowledge (technical, organizational, decisional and human aspects) for obtaining a complete risk, reliability or maintenance analysis. It allows also to calculate exactly the probability of failure

Table 5
Overview of the modeling aspects in maintenance area.

Items	Main contributions	Theoretical contribution	Methodological contribution	Applicative contribution
Covered aspects				
As previously mentioned, there are few covered aspects since it is a recent research field.				
Aspects which researchers are still working on				
Modeling the functional and dysfunctional analysis with impacts on global system performances	Muller et al. (in press)		×	
	Weber and Jouffe (2006)		×	
	Kang and Golay (1999)			×
Including the temporal aspect in maintenance analyses.	Borgia et al. (2009)			×
Modeling the causal relationships between degradation/cause/consequence	Iung et al. (2005)		×	
	De Melo and Sanchez (2008)		×	
Managing models with great number of variables	SKOOB project (2008)			×
Under-developed aspects (*with not transcendental results*)				
Integrating qualitative analysis (functional, dysfunctional and organizational analysis) with quantitative knowledge (technical and financial level)				
Modeling the degradation mechanisms and to represent: the influence factors (service time, age, number of requests, environmental conditions, etc.), the degradation symptoms, the relation between the degradation observation and the appearance of other failure modes, the effects of preventive and corrective maintenance activities, and the planning and execution of maintenance actions				
Modeling the effects of preventive and corrective maintenance activities, and the effect of the planning and the execution of maintenance actions.				
Characterizing, representing and propagating uncertainties (epistemic; random and numeric) in maintenance studies				
Constructing an automated BN model without human expertise.				

of a safety barrier for risk analysis or the probability of failure of an equipment for reliability and maintenance optimization.

Nevertheless, when multiple failures can potentially affect the components with several different consequences on the system (which is usually the case for risk and dependability analyses), the model needs a representation of multiple state variables. In this context, FT are not suitable. Another constraint is that the FT model is limited to assess just one top event. In contrast BN allow similar capabilities to the FT with the advantages of a multi-state variable modeling and the ability to assess several output variables in the same model. Castillo et al. (1997), Portinale and Bobbio (1999) Bobbio et al. (2001, 2003) and Mahadevan et al. (2001) present a relevant contribution in which they explain how FT can be translated to BN, maintaining its Boolean behavior.

So, it is possible to represent FT as BN, but the reciprocity is not true. BN enable the use of multi-modal logic with an unlimited number of modalities and, they make possible and easier the treatment of dependencies based on a DAG (Bouissou and Pourret, 2003). BN can also represent reliability block diagrams. The initial work on this area is presented by Torres-Toledano and Sucar (1998) who explain the translation from one representation to the other. As a consequence, reliability analysis by BN can be based on success paths or by equivalence with minimal cuts or every representation based on Boolean equation.

Recently, some papers have dealt with the link between the new modeling techniques such as dynamic fault trees and BN (Boudali and Dugan, 2005a, 2006). In these papers, the equivalence between dynamic fault trees and BN has been proven. They propose to include the temporal notion on the variables. This technique requires the BN modeling with continuous variables. The dynamic process can be modeled as DBN; also there are several techniques called dynamic fault trees. For instance, the publication by Montani et al. (2006) presents the transformation of a dynamic fault tree into a BN, with a representation of a discrete DBN with 2 time slices (2TBN).

4.2. Markov chains (MC)

A stochastic process can be represented through a group states' description and their transition rate among states. According to the hypotheses assumed for the state transition specifications, the process is Markovian, semi-Markovian or non-Markovian. The representation of the state space is identified on the dependability specialized literature (Aven and Jensen, 1999; Ansell and Phillips, 1994), as well as industrial standards IEC61511 (2004).

This method is suitable for reliability and availability studies of systems. It allows analysis of the exact failure probability even when there are dependencies among components. The MC also allows the integration of diverse kinds of knowledge and to represent multi-state variables. So, they are a relevant tool for the analyses in the fields studied in this paper.

However, in order to explain behaviors and causalities, the systems' modeling becomes complex with a large number of variables. This requirement constitutes the main drawback of MC method since there is a combinatory explosion of the states' number that leads to an unreadable model when studying real industrial systems (De Souza and Ochoa, 1992). With BN there is no longer such a constraint since the number of parameters within the conditional probabilities table is considerably lower compared to a MC.

DBN can represent MC in a compact form. The first contributors on DBN application to the reliability and availability analyses of systems are Welch and Thelen (2000). Then, Weber and Jouffe (2003) have shown the factorization possibility of a Markovian model by DBN. The factorization permits to reduce the model complexity and to open the possibility to model more complex systems.

One main contribution is a DBN representation of non-homogeneous Markovian processes when using changeable parameters through time (Ben Salem et al., 2006). Additionally, Weber et al. (2004) have formalized the inclusion of exogenous variables representing events (maintenance actions, production level, environmental conditions) in a degradation process by using a process called MSM (Markov switching model), or IO-HMM (input–output hidden Markov model). The originality of the proposed approach is to formalize a component's degradation process and its interaction with the environment by an IO-HMM. The models of these processes, interacting with the environment, can be integrated in a system's global model formalized by an object oriented dynamic Bayesian network (OODBN) (Weber and Jouffe, 2006).

4.3. Stochastic Petri networks (SPN)

Stochastic Petri networks (SPN) (Dutuit et al., 1997; Nourelfath and Dutuit, 2004) are now considered as a traditional method to model reliability, availability, etc. SPN are used in the domain of dynamic reliability (Volovoi, 2004) and the maintenance policy optimization (Zouakia et al., 1999). This method is a powerful modeling formalism but unfortunately the reliability analysis is based on a simulation procedure. The dynamic behavior of SPN is analyzed by Monte Carlo simulation or by other variants of this simulation method since the numerical and analytical methods do not enable to deal with non-Markovian processes and the interdependence process resulting from the SPN. Unfortunately, the use of SPN with simulation methods has two disadvantages: inefficient consideration of low-frequency events and the simulation time. The consideration of low-frequency events is an important issue especially in risk analysis since an accident remains a rare event with high consequences. Moreover, SPN do not allow easily integrating evidences. These events could be taken into account with the BN.

BN do not have the same modeling objective as SPN since they are based on a probabilistic inference. In contrast, the SPN are based on the principle of modeling the behavior of processes coupled with a simulation tool and, the extraction of the probabilistic characteristics by statistical analysis.

Even when the final goal of both methods is similar, the way to deal with the issue is very different. Thus, there are few bibliographical references in which can be found a valid comparison or a transformation from SPN to BN. Bobbio et al. (2003) compare BN, FT and SPN in their application to a safety system on a gas turbine. However, this article does not propose a transformation from one representation to another.

One of the possibilities that could be developed is the transformation of a SPN into a DBN. On the one side it is possible to obtain the marked graph from a SPN which could be coded as a Markov Chain. On the other side, the DBN could be transformed into a Markov Chain (as explained in the previous section). This is a clue for the transformation from one method to the other.

5. Conclusion

The research works and applications of Bayesian Networks in risk analysis, dependability and maintenance have shown a significant upward trend since 2000, especially in dependability. Recently, there have been about 30 articles per year and, an increase of 800% of publications between 2000 and 2008. BN in reliability, risk and maintenance areas are chosen since they are easy to use with domain experts. BN are particularly suitable for collecting and representing knowledge on uncertain domains but also enable to perform probabilistic calculus and statistical analyses in an efficient manner.

The difference of BN, in comparison with other classical methods, is their polyvalence. They allow dealing with issues such as prediction or diagnosis, optimization, data analysis of feedback experience, deviation detection and model updating. The graphical representation is interesting since the model complexity is understandable in a single view. In the case of large size model, object oriented representation OOBN or probabilistic relational descriptions (PRM) provide manageable models.

One of the weak points of BN is that there is no specific semantic to guide the model development and to guarantee the model coherence. Therefore, a relevant issue is the use of tools for the formalization of BN models in order to integrate various dimensions (technical, organization, information, decision and finance) correlated with system's behavior in reliability, risk analysis and maintenance fields (Øien, 2001; Kim et al., 2006; Trucco et al., 2008). For solving this issue, the research can follow two directions: The first one concerns the translation of the classical dependability model into a BN model. The second one is to define new methodologies of model development. The first solution leads to a coherent model but is limited by the conditions and hypotheses related to the classical dependability model translated in BN. In opposition, the second approach is more innovative because it leads to a model exploiting all the flexibility of BN formalism but it is difficult to prove the result consistence by comparison with other methods classically based on restrictive hypotheses.

In addition, since there is no specific semantic to build a BN, it is necessary to verify the models and to validate them in accordance with the system reality. One aspect to be developed is formalizing some methods for the sensibility analysis of a model in order to investigate its robustness according to the problem studied (Pollino et al., 2007).

When exploiting a DBN model, there are several inference algorithms that are appropriated to different situations. For example, with the exact inference algorithm proposed by Jensen (1996), the 2TBN model is similar to a Markovian model with dynamic independent variables. It means that when calculating variables at step $(i+1)$, the past before step (i) is forgotten thanks to the Markov property. Thus, the inference using junction tree computes the exact distribution if the variable of the dynamic processes respect the Markov property and no dependency exists between the processes. In this particular case, the results are only exactly the same as the computation in the unroll-up BN model. In that sense, one of the research directions is to guide the use of BN taking into account the limitations of the current inference algorithms in order to warn the community on the possible erroneous use in the models with the temporal aspect. For these representations, several inference algorithms exist and are still in development. Their efficiency depends on the model complexity (Murphy, 2002).

In the dependability analysis there are different phenomena of diverse natures that should be considered i.e. discrete and continuous variables. For this reason a lot of work has been developed in this area in order to integrate continuous variables in BN models. As a result, a significant part of the community is directing its efforts on the development of inference algorithms for hybrid BN (Boudali and Dugan, 2006; Neil et al. 2009; Langseth et al., 2009).

An interesting issue would be to deal with large systems (several hundred variables) in order to formalize complex models. For example, the SKOOB project is developing a generic model based on PRM (Getoor et al., 2007), which enables a better understanding of complexity and the reutilization of generic parts of a model to represent systems. The network is not defined by a graph but in a language. The inference is performed through partial views of the global model which is actually never built entirely as it is approached in SKOOB project (SKOOB, 2008).

Another interesting issue is the manipulation of the imprecision within the parameters and the knowledge of the model (uncertainty). The theory of Dempster Shafer proposes a relevant formalism, and the definition of evidential networks developed by Simon and Weber (2009a, b) are suitable for decision making, considering the imprecision on the utility computation.

As a final point, BN are limited by the modeling aspects that they can deal with. Thus, it is necessary to make BN interoperable with other dependability/risk tools in order to complement the capabilities of BN to better represent the characteristics of a system.

Acknowledgements

The authors wish to express their gratitude to the French National Research Agency (ANR) for the financial support of the Structuring Knowledge with Object Oriented Bayesian nets (SKOOB) project. Ref. ANR PROJET 07 TLOG 021 (http://skoob.lip6.fr). Special thanks are also paid to S. Montani and A. Bobbio from the Università del Piemonte Orientale for their valuable comments during the writing of this article.

References

Alsyouf, I., 2007. The role of maintenance in improving companies' productivity and profitability. International Journal of Production Economics 105, 70–78.
Ansell J.I., Phillips M.J. (1994). Practical methods for reliability data analysis. Oxford University Press Inc. 0 19 853664 X.
Arroyo, G., Sucar, L., Villavicencio, A., 1998. Probabilistic temporal reasoning and its application to fossil power plant operation. Expert Systems with Applications 15, 317–324.
Aven, T., Jensen, U., 1999. Stochastic Models in Reliability. In: Karatzas, I., Yor., M. (Eds.), Applications of mathematics: 41. Springer-Verlag, ISBN: 0-387-98633-2, pp. 1999 SPIN 10695247.
Axel B., Helminen A., 2001. A Bayesian belief network for reliability assessment. SAFECOMP 2001, LNCS 2187, pp. 35–45.
Bai, C.G., 2005. Bayesian network based software reliability prediction with an operational profile. Journal of Systems and Software 77 (2), 103–112.
Bai, C.G., Hu, Q.P., Xie, M., Ng, S.H., 2005. Software failure prediction based on a Markov Bayesian network model. Journal of Systems and Software 74 (3), 275–282.
Bayraktarli Y., Ulfkjaer J., Yazgan U., Faber M., 2005. On the application of bayesian probabilistic networks for earthquake risk management. In: Proceedings of the Ninth International Conference on Structural Safety and Reliability (ICOSSAR 05), Rome, June 20-23.
Bazovsky, I., 1961. Reliability Theory and Practice. Prentice Hall.
Ben Salem A., Muller A., Weber P., 2006. Dynamic Bayesian Networks in system reliability analysis. In: Proceedings of the Sixth IFAC Symposium on Fault Detection, Supervision and Safety of technical processes, 481-486.
Bobbio, A., Montani, S., Portinale, L., 2003. Parametric dependability analysis through probabilistic horn abduction. UAI 2003, 65–72.
Bobbio, A., Portinale, L., Minichino, M., Ciancamerla, E., 2001. Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. Reliability Engineering and System Safety 71 (3), 249–260.
Borgia, O., De Carlo, F., Peccianti, M., Tucci, M., 2009. The Use of Dynamic Object Oriented Bayesian Networks in Reliability Assessment: a Case Study. Recent Advances in Maintenance and Infrastructure Management. Springer-Verlag London Limited, London, England.
Boudali H., Dugan J.B., 2005a. A new Bayesian network approach to solve dynamic fault trees. In: Proceedings of the IEEE Reliability and Maintainability Symposium. 451–456, January 24–27.
Boudali, H., Dugan, J.B., 2005b. A discrete-time Bayesian network reliability modeling and analysis framework. Reliability Engineering and System Safety 87 (3), 337–349.
Boudali, H., Dugan, J.B., 2006. A continuous-time Bayesian network reliability modeling and analysis framework. IEEE Transaction on Reliability 55 (1), 86–97.
Bouissou, M., Pourret, O., 2003. A Bayesian belief network based method for performance evaluation and troubleshooting of multistate systems. International Journal of Reliability, Quality and Safety Engineering 10 (4), 407–416.
Bouissou M., Martin F., Ourghanlian A. (1999). Assessment of a safety critical system including software: a Bayesian belief network for evidence sources. In: Reliability and Maintainability Symposium (RAMS'99). Washington, January 1999.
Castillo, E., Solares, C., Gomez, P., 1997. Tail uncertainty analysis in complex systems. Artificial Intelligence 96, 395–419.
Celeux, G., Corset, F., Lannoy, A., Ricard, B., 2006. Designing a Bayesian network for preventive maintenance from expert opinions in a rapid and reliable delay. Reliability Engineering and System Safety 91 (7), 849–856.
Cheon, S.-P., Kim, S., Lee, S.-Y., Chong-Bum, Lee, 2009. Bayesian networks based rare event prediction with sensor data. Knowledge-Based Systems 22 (5), 336–343.
Cornalba, C., Giudici, P., 2004. Statistical models for operational risk management. Physica A 338, 166–172.
De Melo A.C.V., Sanchez A.J., 2008. Software maintenance project delays prediction using Bayesian Networks. Expert Systems with Applications, Volume 34, Issue 2. Pages 908–919. In Press, ISSN:0957-4174.
De Souza, E., Ochoa, P.M., 1992. State space exploration in Markov models. Performance Evaluation Review 20 (1), 152–166.
Delmotte F., 2003. A socio-technical framework for the integration of human and organizational factors in project management and risk analysis. Master of Science, Faculty of the Virginia Polytechnic Institute and State University.
Doguc, O., Ramirez-Marquez, J.E., 2009. A generic method for estimating system reliability using Bayesian networks. Reliability Engineering and System Safety 94 (2), 542–550.
Duijm, N.J., 2009. Safety-barrier diagrams as a safety management tool. Reliability Engineering and System Safety 94 (2), 332–341.
Dutuit, Y., Chatelet, E., Signoret, J.P., Thomas, P., 1997. Dependability modelling and evaluation by using stochastic Petri nets: application to two test cases. Reliability Engineering and System Safety 55, 117–124.
Embrey D., 2002. Using influence diagrams to analyse and predict failures in safety critical systems. In: Proceedings of the 23rd ESReDA Seminar—Decision Analysis: Methodology and Applications for Safety of Transportation and Process Industries. Delft, The Netherlands, November 2002.
Friis-Hansen, A., Hansen, P., 2008. Reliability analysis of upheaval buckling-updating and cost optimization. ORBIT.
Getoor, L., Friedman, N., Koller, D., Pfeffer, A., Taskar, B., 2007. Probabilistic Relational Models. In: Getoor, L., Taskar, B. (Eds.), Introduction to Statistical Relational Learning. MIT Press, USA, pp. 139–144.
Griffith, W.S., 1980. Multistate reliability models. Journal of Applied Probability 17, 735–744.
Gulvanessian, H., Holicky, M., 2001. Determination of actions due to fire: recent developments in Bayesian risk assessment of structures under fire. Building Research Establishment, Garston, Watford, UK. Klokner Institute, Prague, Czech Republic.
Hanea, D., Ale, B., 2009. Risk of human fatality in building fires: a decision tool using Bayesian networks. Fire Safety Journal 44 (5), 704–710.
Helminen A., Pulkkinen U., 2003. Reliability assessment using Bayesian network—case study on quantitative reliability estimation of a software-based motor protection relay. VTT Industrial Systems. STUK-YTO-TR 198, Helsinki.
Hudson L., Ware B., Laskey K., and Mahoney S., 2002. An application of Bayesian networks to antiterrorism risk management for military planners. Technical Report. Digital Sandbox, Inc.
IEC61025, 2006. Fault tree analysis (FTA). Geneva, IEC.
IEC61511, 2004. Functional safety—safety instrumented systems for the process industry sector, Geneva, IEC.
Iung, B., Veron, M., Suhner, M., Muller, A., 2005. Integration of maintenance strategies into prognosis process to decision making aid on system operation. Annals of the CIRP 54 (1), 5–8.
Jensen, F.V., 1996. An Introduction to Bayesian Networks. Editions UCL Press, London, UK.
Kang, C.W., Golay, M.W., 1999. A Bayesian belief network-based advisory system for operational availability focused diagnosis of complex nuclear power systems. Expert Systems with Applications 17, 21–32.
Kim, M.C., Seong, P.H., Hollnagel, E., 2006. A probabilistic approach for determining the control mode in CREAM. Reliability Engineering and System Safety 91 (2), 191–199.
Kim, M.C., Seong, P.H., 2006. A computational method for probabilistic safety assessment of I&C systems and human operators in nuclear power plants. Reliability Engineering and System Safety 91 (5), 580–593.
Kutucuoglu, K., Hamali, J., Irani, Z., Sharp, J., 2001. A framework for managing maintenance using performance measurement systems. International Journal of Operations and Production Management **21** (1/2), 173–194.
Labeau, P.E., Smidts, C., Swaminathan, S., 2000. Dynamic reliability: towards an integrated platform for probabilistic risk assessment. Reliability Engineering and System Safety 68, 219–254.
Lai, C.-D., Xie, M., 2006. Stochastic Ageing and Dependence for Reliability. Springer, New York.
Langseth, H., 2008. Bayesian Networks in Reliability: The Good, the Bad and the Ugly. Advances in Mathematical Modeling for Reliability. IOS Press, Amsterdam, Netherland.
Langseth, H., Nielsen, T.D., Rumí, R., Salmerón, A., 2009. Inference in hybrid Bayesian networks. Reliability Engineering and System Safety 94, 1499–1509.
Langseth, H., Portinale, L., 2007. Bayesian networks in reliability. Reliability Engineering and System Safety. 92 (1), 92–108.
Lee, C., Lee, K.J., 2006. Application of Bayesian network to the probabilistic risk assessment of nuclear waste disposal. Reliability Engineering and System Safety. 91, 515–532.
Léger A., Farret R., Duval C., Levrat E., Weber P., Iung B., 2008. A safety barriers-based approach for the risk analysis of socio-technical systems. In: 17th IFAC World Congress, Republic of Korea.
Léger, A., Weber, P., Levrat, E., Duval, C., Farret, R., Iung, B., 2009. Methodological developments for probabilistic risk analyses of socio-technical systems. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability 223 (4/2009), 313–332.
Leveson, N., Dulac, N., Marais, K., Carroll, J., 2009. Moving beyond normal accidents and high reliability organizations: a systems approach to safety in complex systems. Organization Studies 30 (2&3), 91–113.
Mahadevan, S., Zhang, R., Smith, N., 2001. Bayesian networks for system reliability reassessment. Structural Safety 23 (3), 231–251.
Mengshoel O.J., Darwiche A., and Uckun S., 2008. Sensor validation using Bayesian networks. In: Proceedings of the Ninth International Symposium on Artificial Intelligence, Robotics, and Automation in Space (iSAIRAS- 08), Los Angeles, CA.
Modarres, M., Kaminskiy, M., Krivtsov, V., 1999. Reliability engineering and risk analysis. Marcel Dekker, New York.
Montani S., Portinale L., Bobbio A., Varesio M., Codetta-Raiteri D., 2006. A tool for automatically translating Dynamic Fault Trees into Dynamic Bayesian

Networks. In: Reliability and Maintainability Symposium (RAMS 2006), pp. 434–441.
Muller A., Suhner M.-C., Iung B., 2008. Formalisation of a new prognosis model for supporting proactive maintenance implementation on industrial system. Reliability Engineering and System Safety. In Press, 93(2), pp. 234–253.
Murphy K., 2002. Dynamic Bayesian Networks: Representation, Inference and Learning. Ph.D. University of California, Berkeley, USA.
Neil, M., Marquez, D., Fenton, N., 2009. Improved reliability modeling using Bayesian networks and dynamic discretisation. Reliability Engineering and System Safety 95 (4), 412–425.
Neil, M., Tailor, M., Marquez, D., Fenton, N., Hearty, P., 2008. Modeling dependable systems using hybrid Bayesian networks. Reliability Engineering and System Safety 93 (7), 933–939.
Norrington, L., Quigley, J., Russel, A., Van der Meer, R., 2007. Modeling the reliability of search and rescue operations with Bayesian Belief Networks. Reliability Engineering and System Safety 93 (7), 940–949.
Nourelfath M. ; Dutuit Y. ; 2004A combined approach to solve the redundancy optimization problem for multi-state systems under repair policies, Reliability Engineering & Systems Safety 0951-8320.
Øien, K., 2001. A framework for the establishment of organizational risk indicators. Reliability Engineering and System Safety 74, 147–168.
Papazoglou, I.A., Bellamy, J.L., Hale, A.R., Aneziris, O.N., Ale, B.J.M., Post, J.G., Oh, J.I.H., 2003. I-Risk: development of an integrated technical and management risk methodology for chemical installations. Journal of Loss Prevention in the Process Industries 16-6, 575–591.
Parida, Aditya, 2006. Development of a multi-criteria hierarchical framework for maintenance performance measurement: concepts, issues and challenges, Division of Operations and Maintenance Engineering. Luleå University of Technology, Luleå.
Pearl, J., 1988. Probabilistic reasoning in intelligent systems: networks of plausible inference. Morgan Kaufmann Publishers Inc, San Francisco, USA.
Perrow C., 1990. Normal Accidents: Living with High-Risk Technologies.
Pollino, C.A., Woodberry, O., Nicholson, A., Korb, K., Hart, B.T., 2007. Parameterisation and evaluation of a Bayesian network for use in an ecological risk assessment. Environmental Modelling and Software 22 (8), 1140–1152.
Portinale L., Bobbio A., 1999. Bayesian networks for dependability analysis: an application to digital control reliability. In: Proceedings of the 15th conference on uncertainty in artificial intelligence. San Francisco, CA: Morgan Kaufmann Publishers; p. 551–8.
Portinale L., Raiteri D.C., Montani S., 2010. Supporting reliability engineers in exploiting the power of Dynamic Bayesian Networks. International Journal of Approximate Reasoning, 51 (2), 179–195.
Pourret, O., Naïm, P., Marcot, B., 2008. Bayesian Belief Networks: A Practical Guide to Applications. John Wiley.
Robert, K., 1990. Managing high reliability organizations. California Management Review, 101–114.
Røed, W., Mosleh, A., Vinnem, J.E., Aven, T., 2008. On the use of hybrid causal logic method in offshore risk analysis. Reliability Engineering and System Safety 94 (2), 445–455.
Simon, C., Weber, P., 2009a. Imprecise reliability by evidential networks. Proceedings of the Institution of Mechanical Engineers Part O Journal of Risk and Reliability 223 (2), 119–131.
Simon, C., Weber, P., 2009b. Evidential networks for reliability analysis and performance evaluation of systems with imprecise knowledge. IEEE Transactions on Reliability 58 (1), 69–87.
Simon, C., Weber, P., Evsukoff, A., 2008. Bayesian network inference algorithm to implement Dempster Shafer theory in reliability analysis. Reliability Engineering and System Safety 93 (7), 950–963.
SKOOB 2008, Structuring Knowledge with Object Oriented Bayesian nets (SKOOB) project. Ref. ANR PROJET 07 TLOG 021 〈http://skoob.lip6.fr〉.
Straub D. (2005). Natural hazards risk assessment using Bayesian networks. In: Proceedings of the Ninth International Conference on Structural Safety and Reliability (ICOSSAR 05), Rome, Italy, June 19–23.
Tavakkoli-Moghaddam, R., Safari, J., Sassani, F., 2008. Reliability optimization of series–parallel system with a choice of redundancy strategies using a genetic algorithm. Reliability Engineering and System Safety 93.
Torres-Toledano J.G., Sucar L.E., 1998. Bayesian Networks for Reliability Analysis of Complex Systems. Lecture Notes In Computer Science; Vol. 1484. Proceedings of the 6th Ibero-American Conference on AI: Progress in Artificial Intelligence. Pages: 195–206, ISBN:3-540-64992-1.
Trucco, P., Cagno, E., Ruggeri, F., Grande, O., 2008. A Bayesian belief network modelling of organisational factors en risk analysis: a case study in maritime transportation. Reliability Engineering and System Safety 93 (6), 845–856.
Villemeur A., 1992. Reliability, Availability, Maintainability and Safety Assessment, Volume 1: Methods and Techniques, volume 1.
Volovoi, V.V., 2004. Modeling of system reliability using petri nets with aging tokens. Reliability Engineering and System Safety 84 (2), 149–161.Waeyenbergh, G., Pintelon, L., 2004. Maintenance concept development: a case study. International Journal of Production Economics 89 (3), 395–405.
Weber, P., Jouffe, L., 2003. Reliability modeling with dynamic Bayesian networks. Reliability Engineering and System Safety. 91 (2), 149–162.
Weber, P., Jouffe, L., 2006. Complex system reliability modeling with dynamic object oriented Bayesian networks (DOOBN). Reliability Engineering and System Safety 91 (2), 149–162.
Weber P., Munteanu P., Jouffe L., 2004. Dynamic Bayesian Networks modelling the dependability of systems with degradations and exogenous constraints. In: Proceedings of the 11th IFAC Symposium on Information Control Problems in Manufacturing (INCOM'04). Salvador-Bahia, Brazil, April 5–7.
Weber P., Suhner M.-C., Iung B., 2001. System approach-based Bayesian Network to aid maintenance of manufacturing process. In: Proceedings of the Sixth IFAC Symposium on Cost Oriented Automation, Low Cost Automation. Berlin, Germany, 33–39, October 8–9.
Weick, K., Kathleen, M., Sutcliffe, 2001. Managing the Unexpected—Assuring High Performance in an Age of Complexity. Jossey-Bass, San Francisco, CA, USA, pp. 10–17.Welch R.L., 2001. BOLARR: A software product for Bayesian online assessment of reliability and risk, NSF SBIR award 1761391, Phase I Final Report, Gensym Corporation.
Welch, R., Thelen, T., 2000. Dynamic reliability analysis in an operational context: the Bayesian network perspective. In: Smidts, C., Devooght, J., Labeau, P.E. (Eds.), Dynamic reliability: future directions. Maryland, USA, ISBN: 0 9652669 3 1.
Wilson, A.G., Huzurbazar, A.V., 2006. Bayesian networks for multilevel system reliability. Reliability Engineering and System Safety 92 (10), 1413–1420.
Zio, E., 2009. Reliability engineering: old problems and new challenges. Reliability Engineering and System Safety 94, 125–141.
Zouakia, R., Bouami, D., Tkiouat, M., 1999. Industrial systems maintenance modelling using Petri nets. Reliability Engineering & System Safety 65 (2), 119–124. doi:10.1016/S0951-8320(98)00093-3 1999.

International Journal of Systems Science
Vol. 42, No. 1, January 2011, 219–233

Taylor & Francis
Taylor & Francis Group

Design of a fault tolerant control system incorporating reliability analysis and dynamic behaviour constraints

F. Guenab[a], P. Weber[a], D. Theilliol[a]* and Y.M. Zhang[b]

[a]*Faculté des Sciences et Techniques, BP 239, Centre de Recherche en Automatique de Nancy, Nancy Université, CNRS, 54506 Vandoeuvre Cedex, France;* [b]*Department of Mechanical and Industrial Engineering, Concordia University, Montreal, Quebec, Canada, H3G 1M8*

(*Received 10 October 2008; final version received 15 October 2009*)

In highly automated aerospace and industrial systems where maintenance and repair cannot be carried out immediately, it is crucial to design control systems capable of ensuring desired performance when taking into account the occurrence of faults/failures on a plant/process; such a control technique is referred to as fault tolerant control (FTC). The control system processing such fault tolerance capability is referred to as a fault tolerant control system (FTCS). The objective of FTC is to maintain system stability and current performance of the system close to the desired performance in the presence of system component and/or instrument faults; in certain circumstances a reduced performance may be acceptable. Various control design methods have been developed in the literature with the target to modify or accommodate baseline controllers which were originally designed for systems operating under fault-free conditions. The main objective of this article is to develop a novel FTCS design method, which incorporates both reliability and dynamic performance of the faulty system in the design of a FTCS. Once a fault has been detected and isolated, the reconfiguration strategy proposed in this article will find possible structures of the faulty system that best preserve pre-specified performances based on on-line calculated system reliability and associated costs. The new reconfigured controller gains will also be synthesised and finally the optimal structure that has the 'best' control performance with the highest reliability will be chosen for control reconfiguration. The effectiveness of this work is illustrated by a heating system benchmark used in a European project entitled intelligent Fault Tolerant Control in Integrated Systems (IFATIS EU-IST-2001-32122).

Keywords: fault tolerant control systems; system reliability; pseudo-inverse method; hierarchical structure; control reconfiguration

1. Introduction

In most conventional control systems, controllers are designed for fault-free systems without taking into account the possibility of fault occurrence. In order to overcome these limitations, modern complex systems use sophisticated controllers which are developed with fault accommodation and fault tolerance capabilities to meet reliability and performance requirements. A fault tolerant control system (FTCS) is a control system that can maintain system performance close to the desirable one and preserves stability conditions not only when the system is in a fault-free case but also in the presence of faulty components in the system, or at least can ensure expected degraded performances that can be accepted as a trade-off (Zhang, Jiang, and Theilliol 2008). Fault tolerant control (FTC) has been motivated by different goals for different applications (Noura, Theilliol, and Sauter 2000; Theilliol, Noura, and Ponsart 2002; Zhang and Jiang 2008). The main goal of FTCS design is to improve reliability and safety of industrial processes and safety-critical systems. Various approaches for FTCS design have been suggested in the literature. Overviews on the development of FTCS have been provided in survey articles by Patton (1997) and Zhang and Jiang (2008), as well as books by Hajiyev and Caliskan (2003), Mahmoud, Jiang, and Zhang (2003), Blanke *et al*. (2006) and Ducard (2009).

Developed methods can be generally categorised into two groups (Patton 1997; Zhang and Jiang 2008): passive and active approaches. Passive FTC deals with a presumed set of process component failures considered in the controller design stage. Active FTC is characterised by an on-line fault diagnosis process and control reconfiguration mechanism. Fault detection and diagnosis (FDD) refers to the task of inferring the occurrence of faults in a system/process and to find their root causes using various knowledge-based and data-based strategies as outlined by quantitative models (Venkatasubramanian, Rengaswamy, Yin,

*Corresponding author. Email: didier.theilliol@cran.uhp-nancy.fr

ISSN 0020–7721 print/ISSN 1464–5319 online

DOI: 10.1080/00207720903513319
http://www.informaworld.com

and Kavuri 2003a), qualitative models (Venkatasubramanian, Rengaswamy, and Kavuri 2003b) and historical data (Venkatasubramanian, Rengaswamy, Kavuri, and Yin 2003c). Several books have been published, for example Gertler (1998) Chen and Patton (1999), Chiang, Russell, and Braatz (2001), Simani, Fantuzzi, and Patton (2003), Isermann (2006), Witczak (2007), and Ding (2008). Based on the information provided by the fault diagnosis module, a control reconfiguration mechanism is designed in order to reduce and compensate for the effects of fault-induced changes in the system. Advanced and sophisticated controllers have been developed along the lines of active FTC, as outlined in Zhang and Jiang (2008). Issues on integration of FDD and FTC have also been discussed in Jiang and Zhang (2006). Among those developments, some publications have introduced reliability analysis for FTCS. Wu (2001a, 2001b) and Wu and Patton (2003) have used Markov models to dictate the system reliability where subsystems are supposed to reach two states: intact (available) or failed (unavailable). Staroswiecki, Hoblos, and Aitouche (2004) proposed a sensor reconfiguration strategy based on physical redundancy where the reliability analysis provides some information for selecting the optimal redundant sensors. In a similar way, He, Wang, and Zhou (2009) have considered the reliability of sensor faults in the filtering design issue. Recently, Guenab, Theilliol, Weber, Ponsart, and Sauter (2005) proposed a FTC strategy for complex systems composed of various subsystems. The FTC method provides an optimal structure in order to achieve desired objectives with highest reliability under a cost constraint or with lowest cost for achieving the reliability goal.

In this article, the dynamic behaviour of the faulty and reconfigured closed-loop system is taken into account in the design of a FTCS. In this context, complex systems are considered as a set of interconnected subsystems. Each subsystem is assigned some local objectives with respect to quality, reliability and dynamic performance. Each subsystem may take several states, and specific controller gains. In the fault-free case, the structure of the control system is defined based on the set of subsystems connected. Once a fault occurs, the faulty subsystems are assumed being able to achieve local objectives at degraded levels. New structures of the system can then be determined based on the degraded objectives. Each possible structure of the system corresponds to reliability and global performance computed from its subsystem properties. The optimal structure is chosen based on the structure that achieves the required global objectives (static and dynamic) with highest reliability. Once the optimal solution is determined, a new structure and a new control law can be exploited in order to achieve the global objectives as close as possible to the nominal one. From the redesign of a controller for each subsystem, the revisited pseudo-inverse method (PIM) developed by Staroswiecki (2005) is used.

The article is organised as follows. Section 2 is dedicated to defining a set of complex systems. Section 3 is devoted to the design of the FTCS under a hierarchical structure. After some definitions are introduced, a solution is developed under a general formulation. A simulation example is considered in Section 4 to illustrate the performance and effectiveness of the proposed method. Finally, concluding remarks are given in the last section.

2. Problem statement

A large class of systems is described by hierarchical structures (Singh and Titli 1978), also called systems with multiple levels, and there are good reasons for organising the control of systems in this way, such as a reduction in the complexity of communication and computation. The considered approach relies on a hierarchical structure with two levels: a global and a local level. Most of the distributed and interconnected systems, such as manufacturing, automated transportation, chemical processes and the automotive industry can be represented under a hierarchical structure with two main levels.

Under the hierarchical control structure assumption, the global level, called coordinator, is designed as an optimal controller. It defines the nominal global objective γ_g^{nom} with the associated local references r_i and computes the global objective γ_g based on the local output y_i of each subsystem s_i. From instance, in a distillation column, the global objective could be the concentration of alcohol in a liquid and the local objectives correspond to the temperature on each stage.

At the local level, the structure is assumed to be composed of n multi-input multi-output subsystems s_i, $i = 1, \ldots, n$, described by a set of linear state-space representations:

$$\begin{cases} \dot{x}_i(t) = A_i x_i(t) + B_i u_i(t) \\ y_i(t) = C_i x_i(t) \end{cases}, \tag{1}$$

where u_i is the control input vector and y_i is the output vector. A_i, B_i and C_i are constant matrices with appropriate dimensions.

Each subsystem s_i has a controller designed for a normal operation with following feedback-feedforward control structure for command tracking:

$$u_i(t) = -K_i^{\text{feedback}} x_i(t) + K_i^{\text{feedforward}} r_i(t), \tag{2}$$

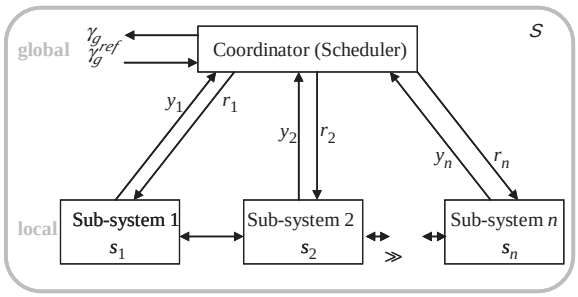


Figure 1. General scheme of hierarchical structure.

where the matrices K_i^{feedback} and $K_i^{\text{feedforward}}$ are synthesised such that the closed-loop behaviour follows the reference model described as follows:

$$\dot{x}_i(t) = M_i x_i(t) + N_i r_i(t), \tag{3}$$

where M_i and N_i matrices are designed in order to describe a desired reference model, which specifies the desired dynamic characteristics of the subsystem under the normal condition.

For a more convenient point of view, subsystems are assumed to be decoupled, which means that matrix A_i is block diagonal. Moreover, subsystem s_i is coupled to subsystem s_{i+1} or inversely.

Figure 1 presents an illustrative scheme of a hierarchical structure.

Due to abnormal operation or material ageing, actuator or component faults can occur in the system. Therefore, the linear state-space model representation defined in (1) may become

$$\begin{cases} \dot{x}_i(t) = A_i^f x_i(t) + B_i^f u_i(t) \\ y_i(t) = C_i x_i(t) \end{cases}, \tag{4}$$

where A_i^f (respectively B_i^f) represents the state (input) matrix in the presence of faults f on the plant/process such as components (actuators).

The occurrence of such faults may result in an unsatisfactory performance and may lead the system to become unstable. Consequently, it is important to design control systems for being able to maintain system performance and reliability. This article aims to design a FTCS in order to maintain nominal or achieve admissible performances despite a fault. A fault detection and isolation (FDI) module is assumed to generate suitable information for control reconfiguration. Before tackling this problem, let us recall the control problem in a general way as suggested by Staroswiecki and Gehin (2001) based on the triplet $\langle \gamma_g, C, U \rangle$, where γ_g are global objectives, C is a set of constraints given by the structure S and parameters Θ of a closed-loop system and U is a set of control laws.

In the fault-free case, the control problem could be solved by a control law $u \in U$ such that the controlled system can achieve the global objectives γ_g under a constraint C. A structure S and parameters Θ are defined and the controller gains of all subsystems and their associated references to achieve the global objectives γ_g are designed. Consequently, the reference global objectives γ_g^{ref} are achieved under the nominal control law u_{nom} with the nominal structure S_{nom}. In a faulty case, the structure S_{nom} is assumed to be modified. Under the presence of faults, the global objectives can be or cannot be achieved under a new structure. In this context, the FTC problem should be able to find a solution to the triplet $\langle \gamma_g, C, U \rangle$. According to a reconfigurability analysis on the distributed and interconnected systems established *a priori* as proposed in Blanke et al. (2006) and associated articles such as Staroswiecki and Gehin (1998), M structures S_m, $m = 1, \ldots, M$, could be considered as reconfigurable ones. A reconfigurable structure consists of changing the structure S_{nom}, parameters Θ and/or control law $u \in U$ of the post-fault system to achieve the global objectives γ_g^{ref}. Among M structures S_m, a solution can be provided by the disconnection or replacement of faulty subsystems. in some cases, no solution may exist, and then global objectives must be redefined to degraded ones, noted as γ_g^d. Then the problem statement is formulated by the following question: how does one choose an optimal structure in the sense that for a given criterion J the selected structure can maintain the objectives γ_g^{ref} (or degraded ones γ_g^d)? This article aims to provide a solution to the above problem based on reliability analysis under dynamic behaviour constraints in the hierarchical structure framework.

3. FTCS design

3.1. *Reliability computation*

Reliability is the ability that units, components, equipment, products and systems will perform their required functions for a specified period of time without failure under stated conditions and specified environments (Gertsbakh 2000). Reliability analysis of components consists of analysing time to a failure from data obtained under normal operating conditions (Cox 1972). In many situations and especially in the considered study, failure rates are obtained from components under different levels of loads: the operating conditions of components change from one structure to another. Several mathematical models have been developed to define the failure level in order to estimate the failure rate λ (Finkelstein 1999; Martorell, Sanchez, and Serradell 1999). The proportional hazards model

introduced by Cox (1972) is used in this article. The failure rate is modelled as follows:

$$\lambda_i(t, \ell) = \lambda_i(t)\, g(\ell, \vartheta), \tag{5}$$

where $\lambda_i(t)$ represents the baseline failure rate (nominal failure rate) function of time for the i-th subsystem/component and $g(\ell, \vartheta)$ is a function (independent of time) taking into account the effects of applied loads with ℓ presenting an image of the load and ϑ defining some parameters of the subsystem/component.

Different definitions of $g(\ell, \vartheta)$ exist in the literature. However, the exponential form is commonly used. Moreover, the failure rate function for the exponential distribution is constant during the useful life but it can change from one operating mode to another according to a load level for the structure S_{nom}. Under these conditions, the failure rate (5) can be rewritten as

$$\lambda_i^m(t, \ell) = \lambda_i(t) e^{\vartheta \times \ell_m}. \tag{6}$$

It can be noticed that load levels (or mean load levels) ℓ_m are assumed constants for the i-th subsystem/component. If an event occurs on the system, based on a novel (or not) load value applied to the component, a new failure rate is calculated. Then the reliability for a period of desired lifetime, noted as T_d, is commonly calculated as follows:

$$R_i^m(T_d) = e^{-\lambda_i^m(T_d, \ell_m) \times T_d}, \tag{7}$$

where $R_i^m(T_d)$ represents the reliability of i-th subsystem used by the structure S_m for the specified time T_d. It should be pointed out that T_d represents the time period between the fault occurrence and the reparation of the faulty component which caused the structure modification.

From complex systems, a global reliability $R_g^m(T_d)$ is computed based on the reliabilities of elementary components or subsystems. Indeed, the global reliability $R_g^m(T_d)$ usually depends on the subsystem's connection which can generally be decomposed on elementary combinations of serial and parallel components. Therefore, the computation of the global reliability $R_g^m(T_d)$ is both based on the reliability of

– n serial subsystems as defined by

$$R_g^m(T_d) = \prod_{i=1}^{n} R_i^m(T_d). \tag{8}$$

– n parallel subsystems as represented by:

$$R_g^m(T_d) = 1 - \prod_{i=1}^{n} (1 - R_i^m(T_d)), \tag{9}$$

where $R_i^m(T_d)$ represents the i-th subsystem reliability.

3.2. *Cost computation*

Let us assume that the system uses all n subsystems. The subsystems' reliabilities are computed at a given time T_d and for each subsystem a cost is associated with it. The objective is to obtain the expected cost of each subsystem as a function of its reliability. Several forms of cost are possible, for example Mettas (2000) and Wu, Wang, Smapath, and Kott (2002). An expected cost function, proposed by Mettas (2000) is used in this article as follows:

$$C_i^m(R_i^m(T_d)) = \frac{\varsigma_i + P}{\int_0^\infty R_i^m(t)\mathrm{d}t}, \tag{10}$$

where ς_i is the initial acquisition cost (price) of i-th subsystem, P is the failure cost due to the performance degradation and $\int_0^\infty R_i^m(t)\mathrm{d}t$ is the mean time to failure of i-th subsystem.

In our case, we propose the formula of the cost over the operating time T_d. At $t = T_d$ there is a probability $(1 - R_i^m(T_d))$ of the component having failed with the associated costs represented by $(\varsigma_i + P)$. This cost is not constant over the operating time T_d. During an interval $[0 \quad T_d]$, the cost is given by

$$C_i^m(R_i^m(T_d)) = \frac{(\varsigma_i + P)(1 - R_i^m(T_d))}{\int_0^{T_d} R_i^m(t)\mathrm{d}t}. \tag{11}$$

The originality of the cost C_i^m is that it is computed according to a desired operating time T_d. Once costs of all subsystems are computed, the cost of the composite system is given by

$$C_g^m = \sum_i C_i^m(R_i^m(T_d)). \tag{12}$$

3.3. *Reconfigurable controller gain synthesis based on an admissible model matching method*

Under the assumption that each multi-input multi-output subsystem s_i $(\forall\, i = 1, \ldots, n)$ defined by Equation (1) or Equation (4) are controllable, the control laws $u_i(t) = -K_i^{\text{feedback}} x_i(t) + K_i^{\text{feedforward}} r_i(t)$ are synthesised such that the closed-loop behaviours are close to a specified reference model $\dot{x}_i(t) = M_i x_i(t) + N_i r_i(t)$, respectively. The controller gains $(K_i^{\text{feedback}}, K_i^{\text{feedforward}})$ are commonly synthesised by solving the following equations:

$$\begin{aligned} A_i - B_i K_i^{\text{feedback}} &= M_i, \\ B_i K_i^{\text{feedforward}} &= N_i, \end{aligned} \tag{13}$$

with a unique solution defined as follows:

$$\begin{aligned} K_i^{\text{feedback}} &= B_i^+ (A_i - M_i), \\ K_i^{\text{feedforward}} &= B_i^+ N_i, \end{aligned} \tag{14}$$

where B_i^+ is the left pseudo-inverse of B_i.

If (13) is not fulfilled, optimal solutions, as presented by Huang and Stengel (1990), should be computed through the following criteria:

$$J_{i1} = \left\| A_i - B_i K_i^{\text{feedback}} - M_i \right\|_F^2, \tag{15}$$

and

$$J_{i2} = \left\| B_i K_i^{\text{feedforward}} - N_i \right\|_F^2, \tag{16}$$

where $\|\cdot\|_F$ represents the Frobenius norm.

Using constrained optimisation, Gao and Antsaklis (1991) synthesised suitable gains based on the PIM which guarantees the closed-loop system stability with successful results in faulty cases for achievable performances where, instead of considering one single reference (closed-loop) behaviour M (respectively N for tracking), a family of reference models $\mathfrak{M}$ (respectively $\mathfrak{N}$ for tracking) that are acceptable are provided. In this article, in order to redesign the controller dedicated to each i-th faulty subsystem, the idea of the recently revisited PIM, developed by Staroswiecki (2005), has been adopted. Under the assumptions that the FDI scheme provides necessary information, the revisited PIM can provide an appropriate controller $(\tilde{K}_i^{\text{feedback}}, \tilde{K}_i^{\text{feedforward}})$ with a degree of freedom for solving Equation (13). As presented in Section 2, the control problem is defined by the triplet $\langle \gamma_g, C, U \rangle$. In faulty cases and for each subsystem, the triplet is equivalent to

$$\begin{aligned} \gamma_i &: \dot{x}_i(t) = M_i x_i(t) + N_i r_i(t), (M_i, N_i) \in \mathfrak{M}_{\text{i}} \times \mathfrak{N}_{\text{i}} \\ C_i &: \dot{x}_i(t) = A_i^f x_i(t) + B_i^f u_i(t) \\ U_i &: u_i(t) = -\tilde{K}_i^{\text{feedback}} x_i(t) + \tilde{K}_i^{\text{feedforward}} r_i(t) \end{aligned}, \tag{17}$$

where (M_i, N_i) are among the sets of admissible reference models $\mathfrak{M}_{\text{i}} \times \mathfrak{N}_{\text{i}}$.

In faulty cases, $\mathfrak{N}_{\text{i}}$ is defined by

$$\mathfrak{M}_i = \left\{ M_i \middle| \phi_{1i}(M_i) \le 0 \quad \text{and} \quad \phi_{2i}(M_i) > 0 \right\}, \tag{18}$$

where functions ϕ_{1i} and ϕ_{2i} describe any matrix M_i which has suitable dynamic behaviour, i.e. stability and appropriate time response. The functions $\phi_{2i}(M_i) > 0$ can be rewritten as $-\phi_{2i}(M_i) < 0$ and (18) is equivalent to a unique function $\phi_i(M_i) < 0$:

$$\mathfrak{M}_{\text{i}} = \left\{ M_i \middle| \quad \phi_i(M_i) \le 0 \right\}. \tag{19}$$

In this article, for simplicity and without loss of generality, the set $\mathfrak{M}_{\text{i}}$ is defined such that any matrix in $\mathfrak{M}_{\text{i}}$ has its eigenvalues lying within a suitable interval. According to the knowledge of the system, this bounded interval is designed in the fault-free condition.

From illustration, an elementary reference model $\dot{x}(t) = Mx(t)$ with its associated eigenvalues being equal to $\tau_1^* = -1$, $\tau_2^* = -1.2$ and $\tau_3^* = -1.4$ is considered. Let the set $\mathfrak{M}$ of admissible reference models be defined by (19) with $\phi(M) \le 0$ corresponding to $\pm 10\%$ of nominal eigenvalues. It can be verified that any matrix belonging to

$$\mathfrak{M} = \left\{ M = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} \middle| \begin{cases} -a-e-i-3.96 \le 0 \\ a+e+i+3.24 \le 0 \\ -bd+ai-gc+ei+ea \\ \quad -fh-5.1788 \le 0 \\ bd-ai+gc-ei-ea+fh \\ \quad +3.4668 \le 0 \\ -gbf+afh+gce+dbi \\ \quad -aei-dch-2.2361 \le 0 \\ gbf-afh-gce-dbi+aei \\ \quad +dch+1.2247 \le 0 \end{cases} \right\}$$

has its eigenvalues $\tau_1 = \beta\tau_1^*$, $\tau_2 = \beta\tau_2^*$ and $\tau_3 = \beta\tau_3^*$ with $\beta = [0.9, 1.1]$.

Similar to $\mathfrak{M}_{\text{i}}$, $\mathfrak{N}_{\text{i}}$ is defined as $\mathfrak{N}_i = \left\{ N_i \middle| \varphi_i(N_i) \le 0 \right\}$.

According to the previous sets of admissible reference models, the control problem is equivalent to finding $(\tilde{K}_i^{\text{feedback}}, \tilde{K}_i^{\text{feedforward}})$ as follows:

$$\begin{cases} \tilde{K}_i^{\text{feedback}} = \arg \min\limits_{\phi_i(M_i) \le 0} \left\| A_i^f - B_i^f K_i^{\text{feedback}} - M_i \right\|_F^2 \\ \tilde{K}_i^{\text{feedforward}} = \arg \min\limits_{\varphi_i(N_i) \le 0} \left\| B_i^f K_i^{\text{feedforward}} - N_i \right\|_F^2 \end{cases}. \tag{20}$$

Compared to Staroswiecki (2005), it should be noted that the admissible model matching problem is handled with the Frobenius norm applied to guarantee both the static and dynamic behaviours of the closed-loop system.

In order to choose the optimal structure and the optimal controller associated with each subsystem among the hierarchical architecture under the reliability constraint, the next subsection is dedicated to defining pertinent indicators for both steady-state and dynamic performances.

3.4. *Performance criteria*

The FTCS should reduce or try to limit the difference between the dynamic and steady-state behaviour of the nominal system and the reconfigured system. The global objective γ_g is allowed to be determined by some algebraic and differential equations, based on local outputs y_i of each subsystem s_i, denoted by f such that

$$\gamma_g = f(y_1, \ldots, y_i, \ldots, y_n),\ i = 1, \ldots, n. \tag{21}$$

The following normalised indicator is proposed to provide a global steady-state performance evaluation of structure S_m:

$$J^m_{\text{steady}} = \left| \frac{\gamma^{\text{nom}}_g - \gamma^m_g}{\gamma^{\text{nom}}_g} \right|, \tag{22}$$

where γ^{nom}_g represents the global objective of the nominal (fault-free) structure S_{nom} and γ^m_g denotes the global objective of the reconfigured system under structure S_m. It can be noticed that the global objective γ_g is computed on-line based on Equation (22).

About the dynamic performance evaluation, the main goal is to obtain the eigenvalues of the reconfigured system close to the nominal ones. Let us consider the normalised error between a nominal and reconfigured i-th subsystem in terms of eigenvalues, then the maximal error of i-th subsystem can be formulated as:

$$\varepsilon^m_i = \max \left| \frac{\tau^{\text{nom}}_j - \tau^m_j}{\tau^{\text{nom}}_j} \right|, j = 1, \ldots, k_i, \tag{23}$$

where each i-th sub-system has k_i eigenvalues τ_j, $j = 1, \ldots, k_i$ for the nominal structure and τ^m_j for the reconfigured structure S_m, which are computed on-line based on synthesised controller gains using Equation (20).

Based on Equation (23), the dynamic performance associated with the reconfigured structure S_m (composed of n_m subsystems) is quantified by the largest normalised error and is then evaluated as follows:

$$J^m_{\text{dyn}} = \max(\varepsilon^m_i),\ i = 1, \ldots, n_m. \tag{24}$$

3.5. *FTCS design*

Consider a nominal system composed of n subsystems: $s_i,\ i = 1, \ldots, n$. Each subsystem has the following properties: a set of local objectives $\gamma_l(s_i)$ (outputs), a set of eigenvalues τ_i and a failure rate $\lambda_i(t, \ell_n)$, with ℓ_n the nominal level of loads of the subsystems. For the sake of simplicity, let us consider only constant failure rates $\lambda_i(\ell_n)$. Without faults, a nominal structure is designed which uses all n subsystems and its nominal global objectives γ^{nom}_g achieved under the local objectives $\gamma_l(s_i)$ of each subsystem.

In faulty cases, M structures $S_m,\ m = 1, \ldots, M$, are assumed to be suitable where each structure S_m contains n_m subsystems: $\left\{ s^m_1 \quad s^m_2 \quad \cdots \quad s^m_{n_m} \right\}$. The main goal of the method is to select a structure among M structures which ensures global objectives γ^m_g close to the nominal case γ^{nom}_g, also without neglected dynamic properties (in terms of reference model, in particular eigenvalues) and for safety reason under some reliability constraints. An optimal structure among the hierarchical architecture will be determined such that it has a minimum performance criterion (27) under the reliability constraints. From a desired time period T_d, the constraint is defined as the reliability larger than a limited value, i.e. $R^m_g(T_d) \geq R^*_g$ and cost $C^m_g \leq C^*_g$, where R^*_g and C^*_g are defined as constant thresholds defined *a priori*.

Then, for each available reconfigured structure S_m, the following procedure needs to be carried out:

At the local level:

(1) For all combined subsystems' references and each subsystem s^m_i new failure rate $\lambda^m_i(\ell_m)$ are computed from their baseline failure rates according to the new applied loads which depend on various local references and a set of local objectives (outputs). $\gamma^m_l(s^m_i)$ are calculated by taking into account the fault magnitude.
(2) New controllers based on the synthesised gains $(\tilde{K}^{\text{feedback}}_i, \tilde{K}^{\text{feedforward}}_i)$ (Equation (20)) are designed and ε^m_i (Equation (23)) are evaluated.
(3) For a given time period T_d, the corresponding reliability $R^m_i(T_d)$ of each subsystem is computed using Equation (7) and the corresponding cost $C^m_i(R^m_i(T_d))$ is calculated using Equation (11).

At the global level:

(1) Each structure S_m involves a new set of global objectives (outputs) γ^m_g as presented in Equation (21).
(2) The reliability $R^m_g(T_d)$ of the system for all structures is computed using Equations (8) and (9).
(3) The cost C^m_g of the system is computed using Equations (11) and (12).

From each reconfigured structure, from Equation (22), a minimum performance of static index $J^m_{\text{steady, opt}}$ is evaluated using

$$J^m_{\text{steady, opt}} = \min_{R^m_g(T_g) \geq R^*_g,\, C^m_g \leq C^*_g} (J^m_{\text{steady}}) \tag{25}$$

and dynamic index J^m_{dyn} is computed using Equation (24).

To determine the optimal solution, the objective of FTCS is to find the structure that has a reliability $R^m_g(T_d) \geq R^*_g$, the cost $C^m_g \leq C^*_g$ and with minimum performance of index J. The criterion J is evaluated using Equations (24) and (25) as follows:

$$\mathsf{J} = \alpha J^m_{\text{steady, opt}} + (1 - \alpha) J^m_{\text{dyn}}, \tag{26}$$

where α is a weighting constant which determines the relative weight placed on the steady-state and dynamic performance.

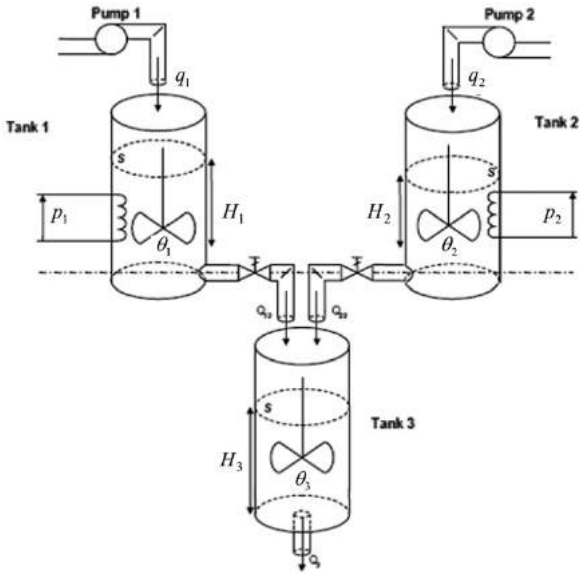


Figure 2. Schematic diagram of the heating system.

Thus the optimal reconfigured structure for a complex system defined as a hierarchical architecture is obtained as follows:

$$S_m^{opt} = \arg \min_{m \; R_g^m(T_g) \geq R_g^*, C_g^m \leq C_g^*} (\mathrm{J}). \tag{27}$$

Once the optimal solution is selected, a new structure S_m^{opt} and a new control law could be exploited in order to satisfy both the local objectives and the corresponding global objectives.

4. Application

The effectiveness and performance of the proposed method are illustrated over a wide range of simulations in the faulty case on a heating system benchmark (Leger, Hamelin, and Sauter 2003). Figure 2 shows the schematic diagram of the entire plant.

4.1. *Process description and control design*

The process is composed of three cylindrical tanks. Two tanks (1 and 2) are used for pre-heating liquids supplied by two pumps. The liquid temperature is adjusted with thermal resistance. A third tank is dedicated for the mixing of the two liquids issued from the pre-heating tanks.

The system instrumentation includes four actuators and six sensors. Control signals p_1, p_2 are powers delivered by the two thermal resistances and q_1, q_2 the input flow rates which are provided by the two pumps. Measurements are liquid temperatures $(\theta_1, \theta_2, \theta_3)$ and

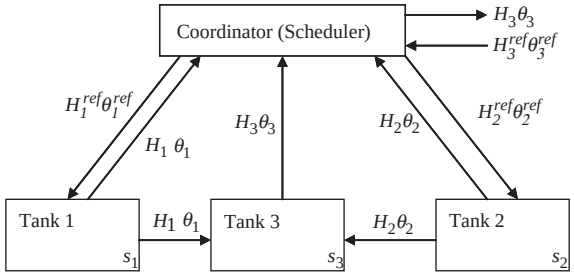


Figure 3. Physical decomposition of the heating system.

liquid levels (H_1, H_2, H_3). A nonlinear system representation is considered to describe the hydraulic and thermal dynamic behaviours in tank 1 and tank 2 such as

$$\begin{cases} \dot{H}_1(t) = & \frac{1}{S}(q_1(t) - \alpha_1\sqrt{H_1(t)}) \\ \theta_1(t) = & \frac{1}{SH_1(t)}\left(\frac{p_1(t)}{\mu c} - (\theta_1(t) - \theta_{1,i})q_1(t)\right) \end{cases}, \tag{28}$$

where S is the tank cross-sectional area, α represents the outflow coefficient, μc corresponds to the thermal constant and finally $\theta_{1,i}$ is the initial condition for the liquid temperature in the tank 1.

According to the instruments available on the heating system in each subsystem s_i, the previous equation can be rewritten as:

$$\begin{aligned} \dot{x}(t) &= f(x(t), u(t)) \\ y(t) &= x(t), \end{aligned} \tag{29}$$

where $x \in \Re^n$ is the state vector, $y \in \Re^m$ is the output vector, $u \in \Re^p$ is the input vector and f a nonlinear function.

According to Equation (29), the system is decomposed into three subsystems such as shown in Figure 3.

The global objectives are to adjust two main reference values: the fluid level H_3^{ref} and the fluid temperature T_3^{ref} in the last tank following static parity equations:

$$H_3 = \left(\frac{\alpha_1\sqrt{H_1} + \alpha_2\sqrt{H_2}}{\alpha_3}\right)^2, \tag{30}$$

$$\theta_3 = \frac{\theta_1\alpha_1\sqrt{H_1} + \theta_2\alpha_2\sqrt{H_2}}{\alpha_3\sqrt{H_3}}. \tag{31}$$

Due to the fact that the process operates in multiple operating regimes, an attractive alternative to nonlinear modelling problem is to use a multi-linear model approach. This approach is successfully used for some nonlinear systems in the control field and consists of partitioning the operating range of a system into separate regions in order to synthesize a global representation. The reader can refer to

Murray-Smith and Johansen (1997) for a comprehensive review on the multiple models strategy, and also for well-developed identification method and modelling problems. A polytopic representation is also used in multi-model representation for nonlinear system modelling and control, as for example in Narendra and Balakrishnan (1997), Tayebi and Zaremba (2002), Ozkan, Kothare, and Georgakis (2003), Wan and, Kothare (2003), Athans, Fekri, and Pascoal (2005) and Toscano and Lyonnet (2006). In this article, the dynamic behaviour of the heating system is assumed to be approximated by a set of N linear time invariant (LTI) models. Consequently, the heating system is formulated as blended multiple models such as

$$\begin{cases} x(t) = \sum_{j=1}^{N} \tilde{G}_j(x(t), u(t))\rho_j(t) \\ y(t) = x(t) \end{cases}, \tag{32}$$

where $\tilde{G}_i$ represents an LTI model established in the vicinity of the j-th equilibrium operating point defined by the set (y_j^e, u_j^e) and ρ denotes a weighting or validity function.

Each LTI model is defined such as

$$\tilde{G}_j(x(t), u(t)) = A_j^o x(t) + B_j^o u(t) + \Delta x_j^o \tag{33}$$

with (A_j^o, B_j^o) being system matrices invariant with appropriate dimensions defined for the j-th operating point, generally established from a first-order Taylor expansion around predefined operating points. Δx_j^o represents a constant vector depending on the j-th linear model and is equal to $\Delta x_j^o = x_j^e - A_j^o x_j^e + B_j^o u_j^e$. It is worthwhile to point out that design of the weighting or validity function ρ is the main task in the multi-model approach. Owing to the main goal of the article, the weighing function ρ is assumed to be assessed directly from output measurements around the j-th operating point as suggested by Toscano and Lyonnet (2006) in a stirred tank reactor.

In the blended multi-model framework, each subsystem s_i has its own associated controller defined for a j-th operating point that implements the following control law:

$$u(t) = -\left(\sum_{j=1}^{N} \tilde{K}_j^{\text{feedback}} \rho_j\right) y(t) + \left(\sum_{j=1}^{N} \tilde{K}_j^{\text{feedforward}} \rho_j\right) r(t), \tag{34}$$

where $\tilde{K}_j^{\text{feedback}}$ and $\tilde{K}_j^{\text{feedforward}}$ are synthesised in order that the closed-loop system follows its reference model.

In the fault-free case, the global objectives are achieved if and if only the reference variables of each subsystem are also reached. This provides a reliability block diagram (RBD) such as shown in Figure 4.

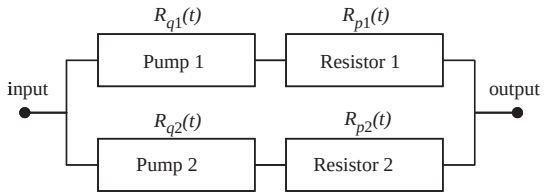


Figure 4. RBD of the heating system.

In the nominal case, the reliability of the entire system is equivalent to $R_g^{\text{nom}}(t) = 1 - (1 - R_{q1}^{\text{nom}}(t) \times R_{p1}^{\text{nom}}(t))(1 - R_{q2}^{\text{nom}}(t) \times R_{p2}^{\text{nom}}(t))$ with a cost function $C_g^{\text{nom}}(t) = C_{q1}^{\text{nom}}(t) + C_{p1}^{\text{nom}}(t) + C_{q2}^{\text{nom}}(t) + C_{p2}^{\text{nom}}(t)$ (see Table A1 for the values of parameters).

4.2. *A set of reconfigured structures*

For illustration purposes, a loss of power in the resistor is considered to occur on the first tank. Three reconfigured structures or working modes are supposed to be involved in the FTCS design.

In the first structure, noted as S_1, only tank 2 and tank 3 are considered in the control loop. The global objectives are achieved without the first tank as

$$H_3 = \left(\frac{\alpha_2\sqrt{H_2}}{\alpha_3}\right)^2, \tag{35}$$

$$\theta_3 = \theta_2. \tag{36}$$

In the second structure, noted as S_2, the heating resistor of the first tank is jammed to its maximal power, i.e. $p_1(t) = (1 - \beta^f) \times p_1^{\max}$. The global objective dedicated to the fluid temperature is affected as follows:

$$\theta_3 = \frac{\theta_1(\beta * p_{\max}^1)\alpha_1\sqrt{H_1} + \theta_2\alpha_2\sqrt{H_2}}{\alpha_3\sqrt{H_3}}. \tag{37}$$

The last one considers, noted as S_3, the nominal structure of the system with an actuator fault. In this working mode, the available local objectives are unlimited.

The reliability and cost functions formula with component failure rates and prices are given in Table A2 for the different structures.

4.3. *Results and analyses*

4.3.1. *Fault-free case*

Different scenarios have been conducted under simulated environments. The validation of the hierarchical controllers under a multiple model framework is shown in Figures 5–7 with respect to fixed global objectives ($H_3^{\text{ref}} = 0.2\,\text{m}$ and $\theta_3^{\text{ref}} = 21^\circ\text{C}$) for a range

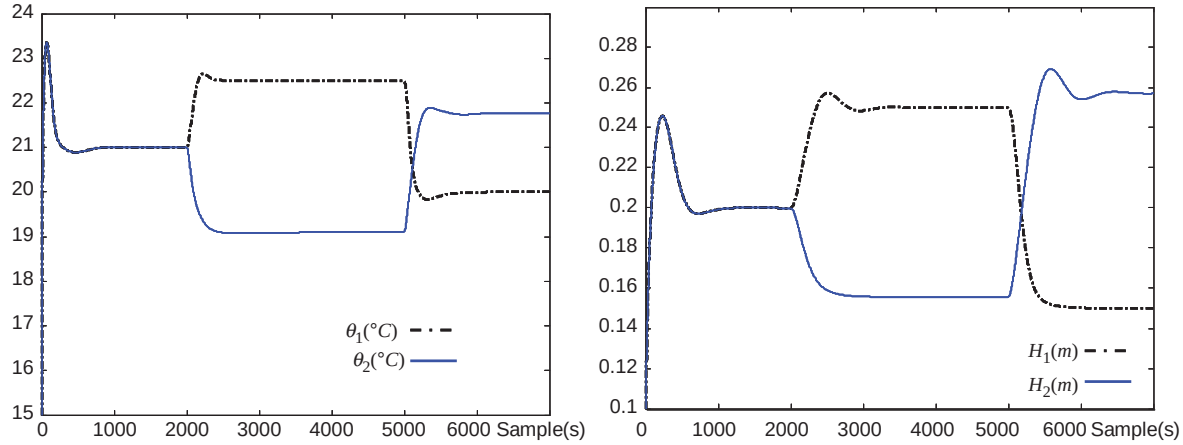


Figure 5. Dynamic evolution of local output variables in the fault-free case.

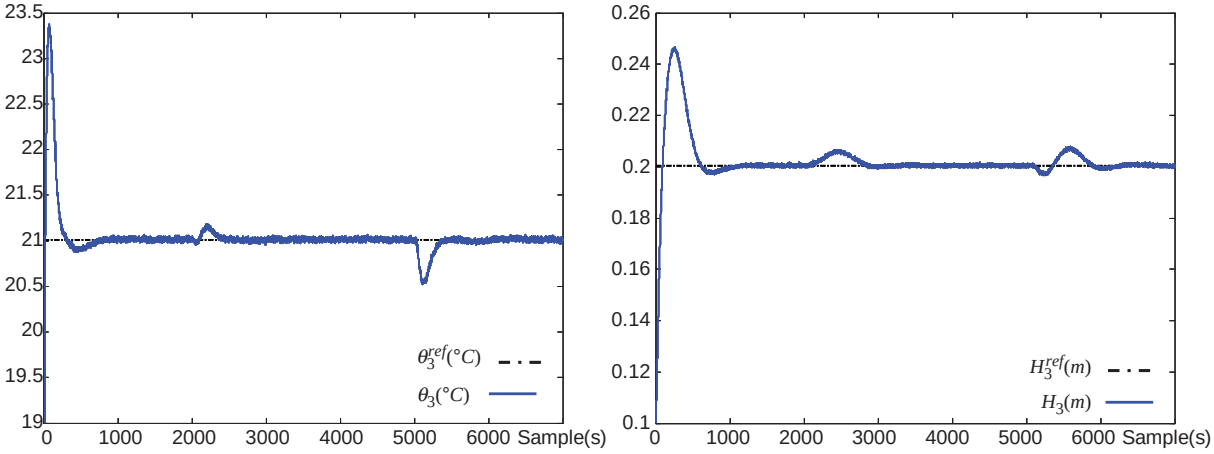


Figure 6. Dynamic evolution of global objectives in the fault-free case.

of 7000 s. Even though some local objectives take several steps and the initial conditions are not close to the reference inputs, the dynamic responses demonstrate that the hierarchical controllers are synthesised correctly (Figure 5). As presented in Figure 6, the fluid level and the fluid temperature in the last tank reach their reference values. The hierarchical controllers preserve the global objective of the system in the presence of step-type reference inputs. Figure 7 shows the corresponding control inputs.

4.3.2. *Actuator fault case without reconfiguration*

A gain degradation of the power in the resistor due to material ageing or a failure, which is equivalent to 70% loss of effectiveness, is supposed to occur at 3500 s. Then, if the output of the controller is equal to P, the power in the resistor applied to the water is equal to $0.3P$ due to the fault. Based on the same controllers as the nominal case, only the local objective θ_1 cannot be achieved for both dynamic and steady-state performances. The consequence of an actuator fault on the local objective is illustrated in Figure 8. The result is that the global objective cannot be achieved, as shown in Figure 9. Due to the fact that the local objectives take several steps, θ_3 is directly affected by the nominal controllers established in the fault-free case: the power designed by the control law in the resistor is saturated as presented in Figure 10. Compared to the dynamic behaviour in the fault-free case, the actuator fault affects only the fluid temperature.

4.3.3. *Actuator fault case with reconfiguration*

The same fault is considered as previously. It is equivalent to a 70% loss of effectiveness occurring at 3500 s. Once the fault is isolated and its magnitude is estimated, the reconfiguration task (FTCS design) is

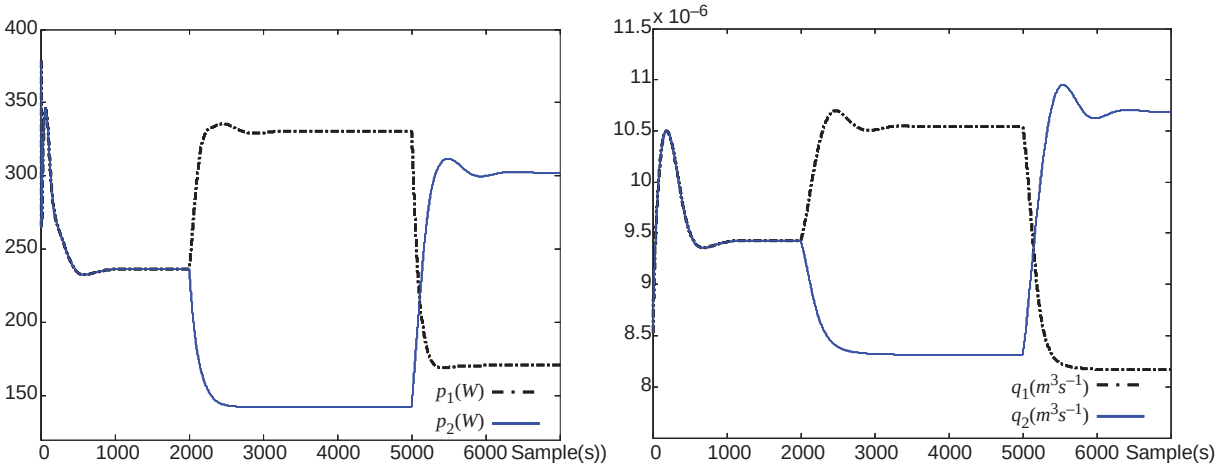


Figure 7. Dynamic evolution of local input variables in the fault-free case.

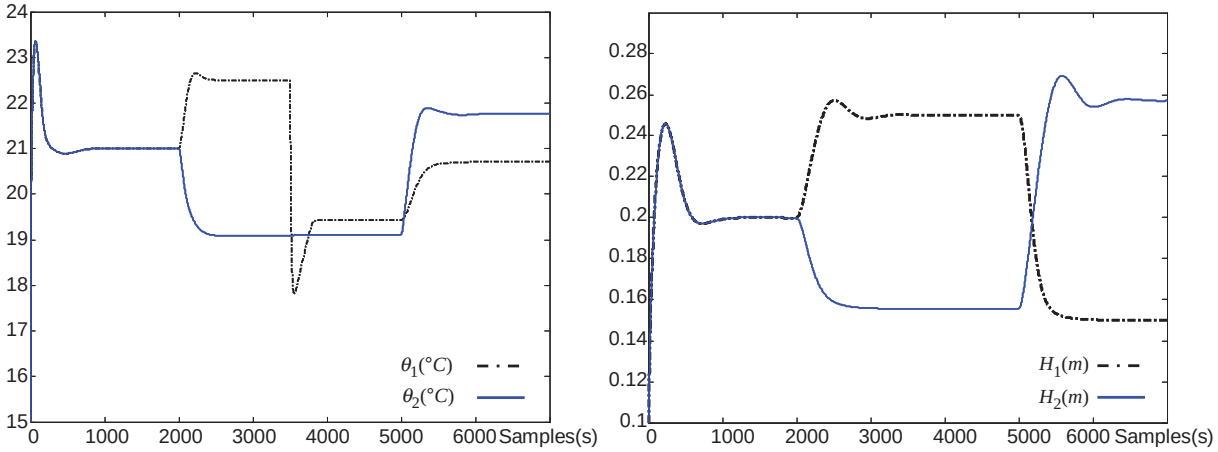


Figure 8. Dynamic evolution of local output variables in the faulty case.

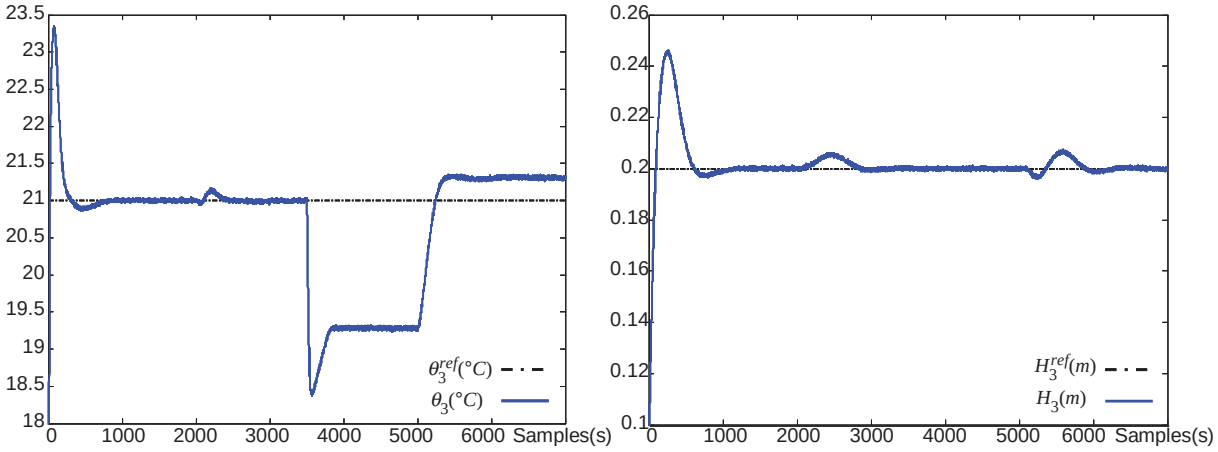


Figure 9. Dynamic evolution of global objectives in the faulty case.

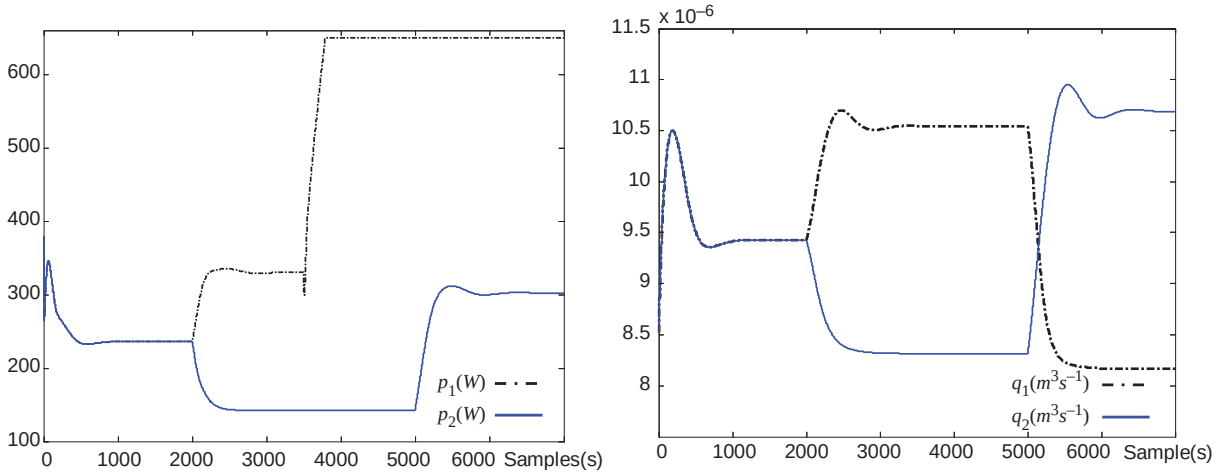


Figure 10. Dynamic evolution of local input variables in the faulty case.

Table 1. Local and global performances of the system under structures S_1, S_2 and S_3.

	S_1	S_2	S_3
H_1	–	0.20	0.1683
θ_1	–	19.9481	17.2711
H_2	0.8	0.20	0.2174
θ_2	20.978	22.023	22.6701
R_{q1}	–	0.9060	0.9129
R_{p1}	–	0.2258	0.7972
R_{q2}	0.76	0.9169	0.9135
R_{p2}	0.79	0.8607	0.8210
C_{q1}	–	0.0188	0.0173
C_{p1}	–	0.2143	0.0326
C_{q2}	0.0427	0.0158	0.0165
C_{p2}	0.0472	0.0255	0.0335
H_3	0.2	0.2	0.1920
θ_3	20.978	20.974	20.1431
J_{steady}	0.001	0.0012	0.0806
J_{dyn}	0	$9.1665*10^{-5}$	$9.1665*10^{-5}$
J	$5.0*10^{-4}$	$1.0583*10^{-3}$	$4.0345*10^{-2}$
C_g	0.0899	0.2743	0.1000
$R_g(T_d)$	0.60	0.8323	0.9319

performed in order to reduce the fault effects on the system and select an optimal structure in order to reach the nominal global objectives.

Table 1 illustrates values of the local and the global objectives of the system, reliabilities and the performance indices for all the structures. The criterion J is defined as $\mathsf{J} = \alpha J^m_{\text{steady, opt}} + (1-\alpha) J^m_{\text{dyn}}$ and it is evaluated using Equations (24), (25) and (26) with $\alpha = 0.5$.

Note that the value of desired reliability is $R^* = 0.55$ and the desired lifetime is $T_d = 10000$ s. According to the constraints R^* and C^* and the performance indices J^m in the structure S_1. Since J^1 has minimal value, it is selected as optimal. Thus, after fault occurrence, the faulty system is switched to the new structure S_1. This leads to the disconnection of the tank 1. The local objectives of tank 2 are applied; they correspond to $\theta_2 = 20.978°\text{C}$ and $H_2 = 0.8$ m, as shown in Figure 11.

The disconnection of tank 1 is carried out by the immediate zero setting of p_1 and q_1 values and closing the connection between tank 1 and tank 3 (Figure 12). This justifies the fall of the level H_3 to 0.05 m, which is equal to $\left(\frac{\alpha_2\sqrt{H_2}}{\alpha_3}\right)^2$ and an increase in temperature θ_3. After transitory duration, the level H_3 and the temperature θ_3 take the values of desired references, as illustrated in Figure 13. These variations of references allow illustration of the effectiveness of the control law p_2 and q_2, which allows reduction of differences between references and actual outputs. The outputs H_2 and θ_2 coincide with the values of references H_2^{ref} and θ_2^{ref}, and the global outputs H_3 and θ_3 coincide with their references. Due to a time delay of a few seconds between fault occurrence and fault diagnosis, the switching procedure generates a time response and an overshoot of the compensated outputs: this dynamic behaviour could be reduced according to a fault diagnosis method. Note that the controller gains of tank 2 are not changed and they take the same values of nominal gains, because the considered fault influences only the disconnected tank (tank 1).

5. Conclusions

This article has presented an FTCS design strategy which can incorporate reliability analysis and performance evaluation into the reconfigurable control structure selection based on the hierarchical architecture of complex systems. Such a strategy requires many computations and is consequently time consuming.

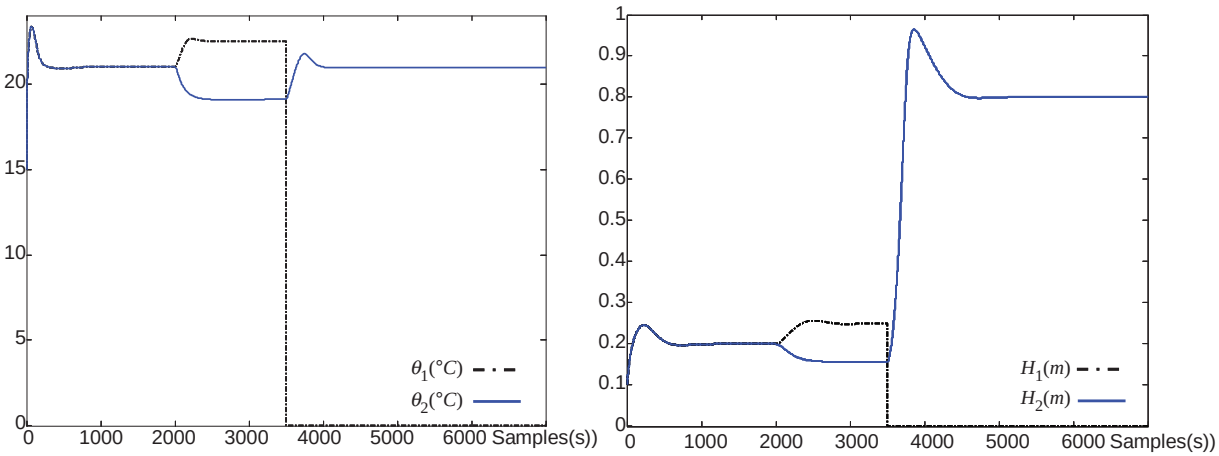


Figure 11. Dynamic evolution of local output variables in the faulty case with FTC.

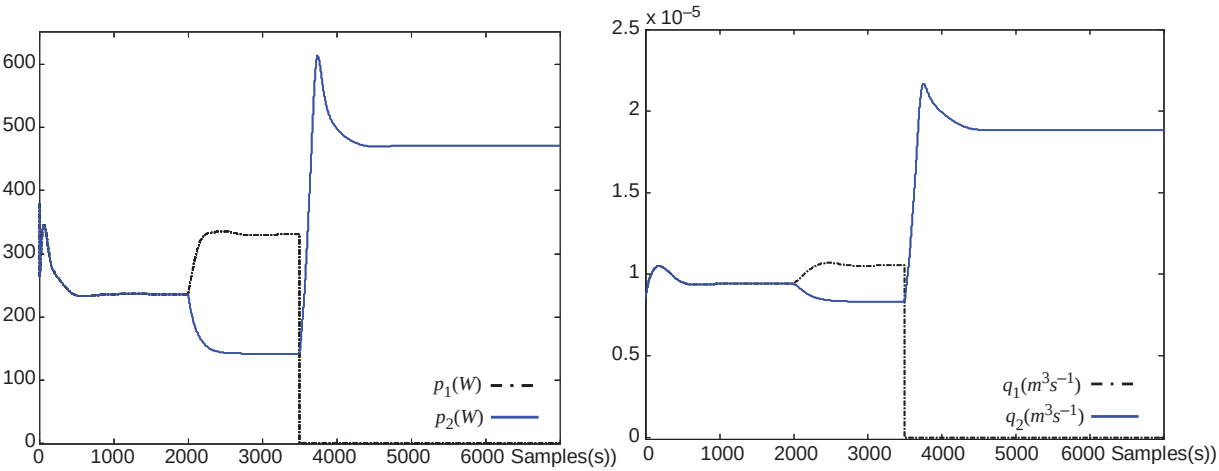


Figure 12. Dynamic evolution of local input variables in the faulty case with FTC.

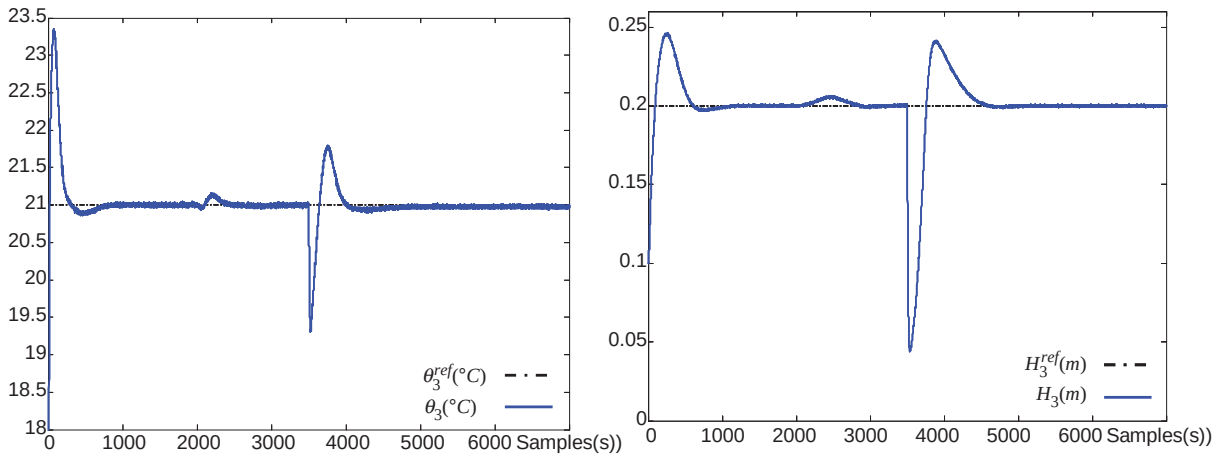


Figure 13. Dynamic evolution of global output variables in the faulty case with FTC.

This constraint can be a limitation in order to apply the developed method to a process with a very low-sampling period. Once a fault occurs and the global objectives of system cannot be achieved using the current structure, the proposed FTC strategy will switch to another structure. The selected structure will guarantee an optimal steady-state and dynamic performance of the reconfigured system according to the 'highest' reliability in order to ensure the dependability of the system and human safety under cost constraints. The effectiveness and performance of the FTCS design strategy have been illustrated on the entire operating conditions of a nonlinear thermal and hydraulic system. Several issues could be investigated in future work. For instance, the proposed approach requires some information about the location, the amplitude and the type of the fault. They are not available unless a FDI module is designed and integrated with the FTCS. Moreover, in order to consider the proposed strategy for processes with a very high sampling period, it is crucial to develop techniques which prove to be less time consuming.

Acknowledgement

Partial support from the European project IFATIS (IFATIS EU-IST-2001-32122) is greatly acknowledged.

Notes on contributors

Fateh Guenab received his State Engineering degree in Automatic Control in 2000 from Setif University, Algeria, his MSc degree in Automatic Control from Institut National Polytechnique de Grenoble, France, in 2003, and his PhD degree in Automatic Control and Signal Processing in 2007 from Henri Poincaré University, Nancy France. Since october 2007, he has occupied a postdoctoral position at Heudiasyc, CNRS Research Unit, Compiègne, France. His research interests are focused on fault tolerant control systems, reconfigurable control systems, safety and reliability of systems.

Philippe Weber received his MS degree in Automatic Control and Signal Processing in 1995 from the University Henri Poincaré, Nancy, France, and his PhD degree in 1999 from Institut National Polytechnique de Grenoble, Grenoble, France. He has been an Assistant Professor at Nancy University since 2000, and a member of the Research Centre for Automatic Control (CRAN) associated with the National Research Centre of Science CNRS (UMR 7039). He focuses his interest on modelling problems in maintenance, prognosis, decision-making processes and dynamic reliability. He develops fault tolerant control systems including reliability analysis. Since 2000 his research interest has been focused on modelling methods based on Bayesian networks.

Didier Theilliol received his PhD degree in Control Engineering from Nancy University (France) in 1993. Since September 2004, he has been a Full Professor in the Research Centre for Automatic Control of Nancy (CRAN) at Nancy-University where he co-ordinates and leads national, European and international R&D projects in steel industries, wastewater treatment plant and aerospace domains. His current research interests include model-based fault diagnosis method synthesis and active fault-tolerant control system design for LTI, LPV, multi-linear systems including reliability analysis. He is a chair of the Intelligent Control and Diagnosis working group where different French and German research teams are involved. He has published over 70 journal and conference articles.

Youmin Zhang received his PhD degree in 1995 from the Department of Automatic Control, Northwestern Polytechnical University, Xian, P.R. China. He held several teaching and research positions in Northwestern Polytechnical University, University of New Orleans, Louisiana State University, State University of New York at Binghamton, the University of Western Ontario, and Aalborg University Esbjerg. He is currently an Associate Professor in the Department of Mechanical and Industrial Engineering at Concordia University, Canada. His current research interests are in the areas of fault diagnosis and fault-tolerant (flight) control systems, cooperative control of unmanned aerial vehicles, dynamic systems modelling, identification and control and signal processing. He has published over 150 journal and conference articles. He is a senior member of AIAA, senior member of IEEE and a member of the IFAC Technical Committee on Fault Detection, Supervision and Safety for Technical Processes.

References

Athans, M., Fekri, S., and Pascoal, A. (20052005), 'Issues on Robust Adaptive Feedback Control', *16th World IFAC Congress*, Prague: Czech Republic.

Blanke, M., Kinnaert, M., Lunze, J., and Staroswiecki, M. (2006), *Diagnosis and Fault-tolerant Control* (2nd ed.), London: Springer-Verlag.

Chen, J., and Patton, R.J. (1999), *Robust Model-based Fault Diagnosis for Dynamic Systems*, Norwell, MA: Kluwer academic.

Chiang, L., Russell, E., and Braatz, R. (2001), *Fault Detection and Diagnosis in Industrial Systems*, New-York: Springer-Verlag.

Cox, D.R. (1972), 'Regression Models and Life Tables', *Journal of the Royal Statistical Society*, 34, 187–220.

Ding, S.X. (2008), *Model-based Fault Diagnosis Techniques – Design Schemes, Algorithms and tools*, London: Springer-Verlag.

Ducard, G.J.J. (2009), *Fault Tolerant Flight Control and Guidance Systems – Practical Methods for Small Unmanned Aerial Vehicles*, London: Springer-Verlag.

Finkelstein, M.S. (1999), 'A Note on Some Ageing Properties of the Accelerated Life Model', *Reliability Engineering and System Safety*, 71, 109–112.

Gao, Z., and antsaklis, P.J. (1991), 'Stability of the Pseudo-inverse Method for Reconfigurable Control Systems', *international Journal of Control*, 53, 717–729.

Gertler, J.J. (1998), *Fault Detection and Diagnosis in Engineering Systems*, New York: Marcel Dekker.

Gertsbakh, I. (2000), *Reliability theory with Applications to Preventive Maintenance*, London: Springer-Verlag.

Guenab, F., Theilliol, D., Weber, P., Ponsart, J.C., and Sauter, D. (2005), 'Fault tolerant Control Method Based on Costs and Reliability analysis', *16th Word IFAC Congress*, Prague: Czech Republic.

Hajiyev, C., and Caliskan, F. (2003), *Fault Diagnosis and Reconfiguration in Flight Control Systems*, Boston: Kluwer Academic.

He, X., Wang, Z., and Zhou, D. (2009), 'Robust H-infinity Filtering for Time-delay Systems with Probabilistic Sensor Faults', *IEEE Signal Processing Letters*, 16, 442–445.

Huang, C.Y., and Stengel, R.F. (1990), 'Restructurable Control Using Proportional-integral Implicit Model Following', *Journal of Guidance, Control and Dynamics*, 13, 303–309.

Isermann, R. (2006), *Fault-diagnosis Systems: An Introduction from Fault Detection to Fault tolerance*, Berlin, Germany: Springer.

Jiang, J., and Zhang, Y.M. (2006), 'Accepting Performance Degradation in Fault-tolerant Control System Design', *IEEE Transactions on Control Systems Technology*, 14, 284–292.

Leger, S., Hamelin, F., and Sauter, D. 'Fault Detection and Isolation Dynamic Systems Using Principal Component Analysis: Application to a Heating System Benchmark,' in *5th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes,* Washington, USA, 2003, pp. 543–547.

Mahmoud, M., Jiang, J., and Zhang, Y.M. (2003), 'Active Fault tolerant Control Systems: Stochastic Analysis and Synthesis', *Lecture Notes in Control and information Sciences* (Vol 287), Berlin, Germany: Springer-Verlag.

Martorell, S., Sanchez, A., and Serradell, V. (1999), 'Age-dependent Reliability Model Considering Effects of Maintenance and Working Conditions', *Reliability Engineering and System Safety*, 64, 19–31.

Mettas, A. Reliability Allocation and Optimization for Complex Systems, in *Proceedings of the annual Reliability and Maintainability Symposium, institute Electrical and Electronics Engineers*, Piscataway, NJ, pp. 216–221, 2000.

Murray-Smith, R., and Johansen, T. (1997), *Multiple Model Approaches to Modelling and Control*, London: Taylor and Francis.

Narendra, K., and Balakrishnan, J. (1997), 'Adaptive Control Using Multiple Models', *IEEE Transactions on Automatic Control*, 42, 171–187.

Noura, H., Theilliol, D., and Sauter, D. (2000), 'Actuator Fault-tolerant Control Design: Demonstration on a Three-tank-system', *international Journal of Systems Science*, 31, 1143–1155.

Ozkan, L., Kothare, M., and Georgakis, C. (2003), 'Control of a Solution Copolymerization Reactor Using Multi-model Predictive Control', *Chemical Engineering Science*, 2, 765–779.

Patton, R.J. *Fault-tolerant Control: The 1997 Situation*, in IFAC Symposium Safeprocess'97, Kingston Upon Hull, UK, pp. 1033–1055, 1997.

Simani, S., Fantuzzi, C., and Patton, R.J. (2003), *Model-based Fault Diagnosis in Dynamic Systems using Identification Techniques*, New York: Springer.

Singh, M.G., and Titli, A. (1978), *Systems Decomposition, Optimisation and Control*, Oxford: Pergamon Press.

Staroswiecki, M., and Gehin, A.L. (1998), 'Analysis of System Reconfigurability Using Generic Component Models', *UKACC Control'98*, Swansea, UK.

Staroswiecki, M., and Gehin, A.L. (2001), 'From Control to Supervision', *Annual Reviews in Control*, 25, 1–11.

Staroswiecki, M., Hoblos, G., and Aitouche, A. (2004), 'Sensor Network Design for Fault tolerant Estimation', *International Journal of Adaptive Control and Signal Processing*, 18, 55–72.

Staroswiecki, M. (2005), 'Fault Tolerant Control: The Pseudo-inverse Method Revisited', *16th Word IFAC Congress*, Prague: Czech Republic.

Tayebi, A., and Zaremba, M. (2002), 'Iterative Learning Control for Non-linear Systems Described by a Blended Multiple Model Representation', *International Journal of Control*, 75, 1376–1384.

Theilliol, D., Noura, H., and Ponsart, J.C. (2002), 'Fault Diagnosis and Accommodation of a Three-tank-system Based on Analytical Redundancy', *ISA Transactions*, 41, 365–382.

Toscano, R., and Lyonnet, P. (2006), 'Robustness analysis and Synthesis of a Multi-PID Controller Based on an Uncertain Multimodel Representation', *Computers and Chemical Engineering*, 31, 66–77.

Venkatasubramanian, V., Rengaswamy, R., Yin, K., and Kavuri, S.N. (2003a), 'A Review of Process Fault Detection and Diagnosis. Part I: Quantitative Model-based Methods', *Computers and Chemical Engineering*, 27, 293–346.

Venkatasubramanian, V., Rengaswamy, R., and Kavuri, S.N. (2003b), 'A Review of Process Fault Detection and Diagnosis. Part II: Qualitative Models-based Methods', *Computers and Chemical Engineering*, 27, 313–326.

Venkatasubramanian, V., Rengaswamy, R., Kavuri, S.N., and Yin, K. (2003c), 'A Review of Process Fault Detection

and Diagnosis: Part III. Process History Based Methods', *Computers and Chemical Engineering*, 27, 327–346.
Wan, Z., and Kothare, M. (2003), 'Efficient Scheduled Stabilizing Model Predictive Control for Constrained Nonlinear Systems', *International Journal of Robust and Nonlinear Control*, 13, 331–346.
Wang, Z., Huang, B., and Unbehauen, H. (1999), 'Robust Reliable Control for a Class of Uncertain Nonlinear State Delayed Systems', *Automatica*, 35, 955–963.
Witczak, M. (2007), 'Modelling and Estimation Strategies for Fault Diagnosis of Non-linear systems: From analytical to Soft Computing Approaches', *Lecture Notes in Control and information Sciences* (Vol 354),Berlin, Germany: Springer.
Eva, N., Wu, X., Wang, Smapath, M., and Kott, G. (2002), 'An Operational Approach to Budget-constrainted Reliability Allocation', in 15th Word IFAC Congress, Barcelona, Spain, pp. 199–204.
Eva Wu, N. (2001a) Reliability of Fault Tolerant Control Systems: Part I, in *40th IEEE Conference on Decision and Control*, Orlando, FL, USA, pp. 1460–1465.
Eva Wu, N. (2001b) Reliability of Fault tolerant Control Systems: Part II, in *40th IEEE Conference on Decision and Control*, Orlando, FL, USA, pp. 1466–1471.
Eva Wu, N., and Patton, R.J. (2003) Reliability and Supervisory Control, in *5th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes*, Washington, DC, USA, pp. 139–144.
Zhang, Y.M., and Jiang, J. (2008), 'Bibliographical Review on Reconfigurable Fault-tolerant Control Systems', *Annual Reviews in Control*, 32, 229–252.
Zhang, Y.M., Jiang, J., and Theilliol, D. (2008), 'Incorporating Performance Degradation in Fault Tolerant Control System Design with Multiple Actuator Failures', *International Journal of Control, Automation, and Systems*, 6, 327–338.

Appendix: Reliability and costs parameters

Table A1. Failure rate (λ), load (ϑ), price (ς) and failure cost (P) parameters.

Component	q_1	p_1	q_2	p_2
$\lambda(\text{hour}^{-1})$	3.77e-6	5.77e-6	3.21e-6	4.25e-6
ϑ	10.211e+4	5.000e-3	10.548e+4	8.000e-3
ς(€)	900	440	820	700
P (€)	1000	1000	1000	1000

Table A2. Reliability (R) and Cost (C) functions.

Structure S_1	$R_g^1(t) = R_{q2}^1(t) \times R_{p2}^1(t)$
	$C_g^1(t) = C_{q2}^1(t) + C_{p2}^1(t)$
Structure S_2	$R_g^2(t) = 1 - (1 - R_{q1}^2(t) \times R_{p1}^2(t))$
	$\times (1 - R_{q2}^2(t) \times R_{p2}^2(t))$
	$\times$ with $p_1(t) = (1 - \beta^f) \times p_1^{\max}$
	$C_g^2(t) = C_{q1}^2(t) + C_{p1}^2(t) + C_{q2}^2(t) + C_{p2}^2(t)$
	$\times$ with $p_1(t) = (1 - \beta^f) \times p_1^{\max}$
Structure S_3	$R_g^3(t) = 1 - (1 - R_{q1}^3(t) \times R_{p1}^3(t))$
	$\times (1 - R_{q2}^3(t) \times R_{p2}^3(t))$
	$C_g^3(t) = C_{q1}^3(t) + C_{p1}^3(t) + C_{q2}^3(t) + C_{p2}^3(t)$

Int. J. Appl. Math. Comput. Sci., 2011, Vol. 21, No. 3, 431–439
DOI: 10.2478/v10006-011-0032-z

RECONFIGURABILITY ANALYSIS FOR RELIABLE FAULT–TOLERANT CONTROL DESIGN

AHMED KHELASSI, DIDIER THEILLIOL, PHILIPPE WEBER

Research Centre for Automatic Control of Nancy (CRAN), CNRS UMR 7039
Nancy University, BP 70239, 54506 Vandœuvre Cedex, France
e-mail: ahmed.khelassi@cran.uhp-nancy.fr

In this paper the integration of reliability evaluation in reconfigurability analysis of a fault-tolerant control system is considered. The aim of this work is to contribute to reliable fault-tolerant control design. The admissibility of control reconfigurability is analyzed with respect to reliability requirements. This analysis shows the relationship between reliability and control reconfigurability defined generally through Gramian controllability. An admissible solution for reconfigurability is proposed according to reliability evaluation based on energy consumption under degraded functional conditions. The proposed study is illustrated with a flight control application.

Keywords: fault-tolerant control system, reconfigurability, reliability, actuator faults.

1. Introduction

Manufacturing systems consist of many different components, which ensure their operation and high-quality production. In order to fulfil the growing of economic demands for high plant availability and system safety, dependability is becoming an essential need in industrial automation. In this context, in order to satisfy these requirements, Fault-Tolerant Control (FTC) is introduced. The aim of FTC systems is to keep a plant available by the ability to achieve the objectives that have been assigned to the system in faulty behavior and accept reduced performances when critical faults occur (Blanke *et al*., 2006). Thus, increasing systems autonomy involves the capability to compensate the impact of component faults and to keep the system available as long as possible. Within this framework, the main goal of FTC is to improve the reliability of the system, which is rarely associated with an objective criterion that guides design (Li *et al*., 2007).

However, it is difficult to establish a functional linkage between the overall system reliability and the control performance requirement.

In active fault-tolerant control, information obtained from fault diagnosis is considered in controller redesign (Noura *et al*., 2009). In fact, process diagnosis should not only indicate fault occurrence but also identify fault location and magnitudes (Tharrault *et al*., 2008). This assumption will make controller re-design possible. After fault occurrence, fault accommodation can be a solution to maintain the performance requirements by adapting the controller parameters (Marusak and Tatjewski, 2008), or by the generation of an additional control law (Blanke *et al*., 2001). Moreover, if fault accommodation cannot be achieved, a complete control loop has to be reconfigured. Then, a new control law has to be designed and the controller structure has to be changed (Zhang and Jiang, 2008). After reconfiguration, the original control objectives are achieved, although degraded performances can be accepted.

Still, the study of the system property is necessary to determine which failure modes could severely affect plant dependability. Only few attempts are focused on fundamental FTC property analysis, where some studies are often defined as fault detectability and fault isolability (Patton, 1997). The concept of reconfigurability was introduced as control system quality under given faulty conditions. In fact, introduced by Moore (1981), the second order mode has been proposed as a reconfigurability measure (Wu *et al*., 2000). LTI system reconfigurability can be also evaluated using the controllability and observability Gramians (Frei *et al*., 1999). In the work of Staroswiecki (2002), performance-based control reconfigurability is evaluated as the ability of the system considered to keep or recover some admissible performances when a fault occurs. Moreover, reconfigurability evaluation is proposed for a general quadratic control problem

by Staroswiecki (2003). Yang (2006) shows that the reconfigurability measure can be viewed as an intrinsic reconfigurability property or as reconfigurability property performance. All these approaches have been considered off-line. Gonzalez-Contreras *et al*. (2009) have recently introduced on-line reconfigurability analysis by using input/output data.

This work contributes to reliable fault-tolerant control systems design which achieves the control objective after fault occurrence with high overall system reliability. Indeed, in order to improve system dependability, reliability analysis is considered to establish an admissible solution of reconfigurability based on the required energy consumption.

This paper is organized as follows. Section 2 formulates the fault-tolerant control problem and defines the reconfigurability concept for actuator faults. Admissibility for fault tolerance is defined according to the energy limitation. In Section 3, reliability estimation in degraded functional conditions is introduced. The impact of actuator faults on reliability is illustrated in order to include the reliability requirements in the reconfigurability problem. A solution for the reconfigurability limit under reliability requirements is proposed to evaluate the ability of the reconfigurable system to recover the encountered faults until the end of the mission. Section 4 is devoted to illustrate this analysis based on an aircraft application. Finally, conclusions are given in the last section.

2. Description of the control reconfigurability problem

2.1. Problem statement. Consider a system in a fault-free case modeled by a linear state-space representation:

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t), \\ y(t) = Cx(t), \end{cases} \tag{1}$$

with the state vector $x(t) \in \mathbb{R}^n$, the control vector $u(t) \in \mathbb{R}^m$, the output vector $y(t) \in \mathbb{R}^r$ and matrices $A \in \mathbb{R}^{n\times n}, B \in \mathbb{R}^{n\times m}, C \in \mathbb{R}^{r\times n}$.

Actuator faults can be defined as any abnormal operations in the control effectors such that the controller outputs cannot be delivered to the manipulated variables entirely. After actuator fault occurrence at $t = t_f$, the control law applied to the plant is interrupted or modified. In this study, the loss of effectiveness control is considered and the system (1) can be represented in the faulty case as follows (Khelassi *et al*., 2010):

$$\begin{cases} \dot{x}(t) = Ax(t) + B_f u(t), \\ y(t) = Cx(t), \end{cases} \tag{2}$$

where the control matrix B_f can be written in relation to the nominal control input matrix B and the control effectiveness factors γ^i, $i = 1, \ldots, m$, as

$$B_f = B(I_m - \Gamma), \quad \Gamma = \begin{pmatrix} \gamma_1 & & & 0 \\ & \gamma_2 & & \\ & & \ddots & \\ 0 & & & \gamma_m \end{pmatrix},$$

with $\gamma_i \in [0 \;\; 1]$. In fact, $\gamma_i = 0$ denotes the healthy i-th control actuator. Nevertheless, when $0 < \gamma_i < 1$, the fault considered is a partial loss in control effectiveness. Moreover, when $\gamma_i = 1$, a failure is considered and the i-th actuator is out of order.

Indeed, the reconfigurability property can be discussed as the ability of the system considered to recover some admissible performances taking into account fault occurrence. According to Yang (2006), reconfigurability can be defined as follows.

Definition 1. The system (1) is called (*completely*) *reconfigurable* if and only if the controllability property of the nominal system is kept by the faulty system.

For an LTI system, reconfigurability evaluation is based on the limitation of energy consumption, which defines an admissible solution in the degraded functional (Staroswiecki, 2002). It can be checked through the controllability Gramian of the system. However, to ensure fault recovery until the end of the mission, fault tolerance evaluation related to actuator reliability can be introduced. In this context, reconfigurability analysis for reliable fault-tolerant control design can be defined based on energy limitation, according to the reliability requirement.

2.2. Reconfigurability based on the controllability Gramian. As proposed by Staroswiecki (2002) and for control reconfigurability analysis, the controllability Gramian appears to be useful in reference to the following: (i) to guarantee the controllability condition of the system proving the existence of a solution; (ii) there exists at least one admissible solution, with respect to some specific energy limitations, taking the system state from $x(0) = x_0 \in \mathbb{R}^n$ to the origin $x(\infty) = 0$.

This problem involves the minimization of the energy consumed by the system. The criterion used is represented as follows.

Criterion 1. Minimize the functional

$$\mathcal{J}(u, x_0) = \int_0^\infty \|u(t)\|^2 \, \mathrm{d}t, \tag{3}$$

to transfer $x(0) = x_0$ to $x(\infty) = 0$, where $x_0 \in \mathbb{R}^n$, and $x(\infty)$ stands for $\lim_{t\to\infty} x(t)$. where $\|\cdot\|$ is the Euclidian norm. Other criteria could be used (see Staroswiecki, 2003).

For the LTI system (1), the solution of (3) is obtained by the Hamiltonian equation from optimal control theory,

$$u(t) = B^T P x(t), \tag{4}$$

where P is the unique solution of the Lyapunov equation defined as

$$A^T P + PA = -BB^T. \tag{5}$$

For the criterion (3), the matrix P^{-1} is the controllability Gramian W_c of the control law $u(t)$. In fact, W_c defines energy consumption required to transfer the system state to the origin. Moreover, W_c is invertible since the pair (A, B) is controllable, defined analytically as follows:

$$W_c = \int_0^\infty e^{At} B B^T e^{A^T t} \mathrm{d}t. \tag{6}$$

The optimal value of the criterion (3) is obtained on $[0, \infty)$ from optimal control theory as follows:

$$\mathcal{J}(x_0) = x_0^T W_c^{-1} x_0. \tag{7}$$

As illustrated by Staroswiecki (2002), Eqn. (7) shows that the actuator performance depends on the control objective x_0. However, actuator performance can be characterized independently of the control objective, which leads to the worst energetic control problem: Transfer the system state $x(0) = x^*$ to $x(\infty) = 0$ where

$$x^* = \arg\max \mathcal{J}(x_0), \tag{8}$$

and the actuator performance is thus evaluated according to the maximum eigenvalue of the matrix W_c^{-1} interpreted as the maximum energy which might be required to transfer the system $x(0) = x^*$ to the origin. The minimum cost associated with (1) in this case can be defined as

$$\mathcal{J}^* = \mathcal{J}(x^*) = \max(\Lambda(W_c^{-1})), \tag{9}$$

where $\Lambda(W_c^{-1})$ is the set of the eigenvalues of W_c^{-1}.

Fault reconfiguration strategies consider the control problem associated with the faulty system. In the degraded functional and for FTC design, the constraint (1) being replaced by the constraint (2) from $t = t_f$,

$$\begin{array}{ll} \dot{x}(t) = Ax(t) + Bu(t), & t \in [0, t_f), \\ \dot{x}(t) = Ax(t) + B_f u(t), & t \in [t_f, \infty). \end{array} \tag{10}$$

Let $\mathcal{J}_f(x_0)$ be the minimum cost of the criterion (3) associated with (10), where the initial condition $x_f = x(t_f)$ is considered on the interval $[t_f, \infty)$. From Bellman's optimality principle, the minimum cost $\mathcal{J}_f(x_0)$ can be obtained in a degraded mode according to the control effectiveness factors γ as

$$\mathcal{J}_f(x_0) = \mathcal{J}_{0f} + x_f^T W_c(\gamma)^{-1} x_f, \tag{11}$$

where $\mathcal{J}_{0f}$ is the cost already spent between $t = 0$ and $t = t_f$. $W_c(\gamma)$ is the solution of the following Riccati equation:

$$AW_c(\gamma) + W_c(\gamma)A^T = -B_f(\gamma)B_f^T(\gamma). \tag{12}$$

In fact, $W_c(\gamma)$ is an invertible and positive matrix, since the pair $(A, B_f(\gamma))$ is kept controllable. The value of $\mathcal{J}_{0f}$ can be expressed as

$$\mathcal{J}_{0f} = \mathcal{J}(x_0) - x_f^T W_c^{-1} x_f. \tag{13}$$

Therefore, the cost associated with the accommodated system can be obtained from (7) and (13) according to the initial conditions as follows:

$$\mathcal{J}_f(x_0) = x_0^T W_c^{-1} x_0^T + x_f^T (W_c(\gamma)^{-1} - W_c^{-1}) x_f. \tag{14}$$

Indeed, for $t_f = \infty$, which defines the lack of occurrence of faults, the associated cost is equal to the nominal case, $x_0^T W_c^{-1} x_0$. However, for $t_f = 0$, fault occurrence is considered when the system is started, and the cost in this case is $x_f^T W_c^{-1}(\gamma) x_f$.

According to Staroswiecki (2002), fault tolerance can be evaluated as follows.

Definition 2. The system is *fault tolerant* with respect to the fault occurring at time $t = t_f$ for the control objective x_0 if and only if the accommodation or the reconfiguration problem has an admissible solution.

Definition 3. In the degraded mode, the solution to the FTC problem is admissible with respect to the control objective x_0 if and only if

$$\mathcal{J}_f(x_0) \leq \mathcal{J}_{\mathrm{pth}}, \tag{15}$$

where $\mathcal{J}_{\mathrm{pth}}$ is a predefined cost corresponding to the worst acceptable degraded mode.

Indeed, admissibility depends on the time of fault occurrence. Since t_f is obviously unknown beforehand, it can only be checked on-line when a fault is detected and isolated. Therefore, it is interesting to look for sufficient conditions which could be checked off-line. Indeed, the control objective can be reached by an admissible solution using the faulty system from the beginning by considering the worst case value of x_f in the previous conditions (Staroswiecki, 2003). The worst case situation is that in which the fault occurrence time is $t_f = 0$. Therefore, $x_f = x_0$ and fault tolerance can be evaluated based on the following indicator:

$$\sigma(\gamma) = \max \Lambda(W_c^{-1}(\gamma)), \tag{16}$$

where $\Lambda(W_c^{-1})$ is the set of the eigenvalues of W_c^{-1}.

Remark 1. The actuator performances can be characterized independently of the control objective by the maximum eigenvalue of $W_c^{-1}(\gamma)$, which is interpreted as the maximum energy required to transfer the system state to the origin. This energy value corresponds to the worst case, which can occur in a given degraded mode.

An index of reconfigurability based on the maximum required energy (16) is proposed by normalization as illustrated by Khelassi *et al*. (2009). Fault tolerance is evaluated by means of the energy cost corresponding to the worst situation in which the system is still controllable for an admissible solution:

$$\rho(\gamma) = \frac{\sigma(\gamma) - \sigma_{\min}}{\sigma_{\max} - \sigma_{\min}}, \tag{17}$$

where $\sigma_{\max}$ is the maximum required energy of the worst degraded functional condition, $\sigma_{\min}$ is the maximum required energy consumed in the nominal situation $\gamma = 0$. Due to the normalization of the energetic indicator (16), the values of the index (17) vary between 0 and 100%. The index (17) can be interpreted as an image of system behavior degradation in terms of energy.

Lemma 1. *In the degraded mode, the solution of the FTC problem is admissible with respect to a control objective if*

$$\rho(\gamma) \leq \rho_{\text{pth}}, \tag{18}$$

where ρ_{pth} is a predefined energetic threshold, which represents the acceptable degraded functional mode when a control solution is found. The value of ρ_{pth} corresponds to an admissible required energy.

Remark 2. The set of admissible solutions which satisfy the relation (18) is established in order to guide the design of a fault tolerant control system. However, the problem is how define the value of the threshold ρ_{pth} based on specified requirements.

In the following section, a solution of the admissibility problem based on the reliability requirement is proposed.

3. Reconfigurability based on reliability analysis

As presented previously, reconfigurability based on the controllability Gramian is applied to evaluate the system performances, which can be achieved by a fault-tolerant control scheme. To improve system dependability, it is crucial to ensure that the reconfigured system can provide the energy required to achieve the control objective until the end of the mission.

Proposition 1. *The mean operating time of the system can be estimated by a reliability measure. For reliable-fault-tolerant control design, the problem (3) can be reformulated as an energetic minimization problem with respect to a reliability requirement such that*

$$J(x_0) = \int_0^\infty \|u(t)\|^2 \, \mathrm{d}t, \tag{19a}$$

subject to

$$R(t) \geq R_{\text{pth}}, \tag{19b}$$

where $R(t)$ is the overall system reliability; R_{pth} is a predefined threshold, which defines the minimal value of the acceptable reliability value in the degraded mode.

The aim of this section is to establish a solution for choosing the admissibility threshold ρ_{pth} based on reliability analysis. In fact, ρ_{pth} is the normalization of a predefined energetic threshold σ_{pth} required to define the acceptable degraded modes which can be tolerated for reliable design.

3.1. Reliability computation.

Definition 4. *Reliability* is defined as the probability that units, components, equipment and systems will accomplish their intended function for a specified period of time under some stated conditions and in specific environments (Gertsbakh, 2000).

In this study, an exponential distribution is considered to model reliability. In fact, reliability evolution is characterized by a given failure rate. Thus, failure rates are obtained from components under different levels of loads. Several mathematical models have been developed to define the load function in order to estimate the failure rate λ (Martorell *et al*., 2009). Among them, the proportional hazard model introduced by Cox (1972) is used in this paper.

Definition 5. The *failure rate* is modeled as follows:

$$\lambda_i = \lambda_i^0 \times g(\ell, \vartheta), \tag{20}$$

where λ_i^0 is the baseline failure rate (nominal failure rate) for the i-th subsystem or component and $g(\ell, \vartheta)$ is a function (independent of time) which models the effects of the employed load on component health. Here ℓ corresponds to the load and ϑ represents some component parameters.

Different definitions of $g(\ell, \vartheta)$ exist in the literature. However, the exponential form, assumed to be related directly to the control input, is commonly used in actuator reliability evaluation. For the nominal functional conditions, Eqn. (20) can be written as follows:

$$\lambda_i = \lambda_i^0 \times e^{\alpha u_{\text{nom}}^i}, \tag{21}$$

where α is a fixed factor depending on the actuator property, u_{nom}^i is the nominal control law delivered by the i-th actuator in the fault-free case to achieve the control objective. Thus, actuator reliability can be evaluated as follows:

$$R_i(t) = e^{-\lambda_i t}. \tag{22}$$

3.2. Reliability evaluation under degraded functional conditions. As explained by Guenab *et al.* (2006), the estimated value of the failure rate changes according to the increase of control input. However, even when actuator faults occur, the control law is modified in order to recover the impact of a fault on system behavior. Thus, the energy required to tolerate the fault increases, and a new failure rate which characterizes actuator reliability degradation and the load can be estimated. In fact, the relationship between the required energy in degraded modes and reliability evolution can be established. Let the linearized dynamics of the normal system at a trim condition be given by (1). Suppose now that one or more actuators are suddenly damaged or experience a partial loss of their control effectiveness (2). Then the system dynamics can be expressed by

$$\dot{y} = C\dot{x} = CAx + CB_f u. \tag{23}$$

At the current state $x(t)$, suppose that the reference baseline system control law for the desired behavior would produce input $u_{\rm nom}$ if all of the control actuators were healthy. Then the desired rate of the controlled output would be

$$\dot{y}_{\rm nom} = C\dot{x} = CAx + CBu_{\rm nom}. \tag{24}$$

FTC seeks an input control u that makes the right-hand side of (23) as close as possible to that of (24), that is,

$$Bu_{\rm nom} = B_f u, \tag{25}$$

where, consequently, y will remain close to $y_{\rm nom}$ for

$$u = (I - \Gamma)^{-1} u_{\rm nom}. \tag{26}$$

Therefore, based on (21) and (26), the failure rate and the reliability of the actuator under degraded functional conditions can be established according to the loss of effectiveness factors γ_i and $u^i_{\rm nom}$ as follows:

$$\lambda_i(\gamma) = \lambda_i^0 e^{(1-\gamma_i)^{-1}\alpha u^i_{\rm nom}}, \tag{27}$$

$$R_i(t,\gamma) = e^{-\lambda_i(\gamma)t}. \tag{28}$$

The overall system reliability depends on the way in which their components and subsystems are connected. In this context, for a system with q series sub systems, reliability is given by

$$R_g(t) = \prod_{i=1}^{q} R_i(t,\gamma), \tag{29}$$

and with q parallel subsystems it is calculated as follows:

$$R_g(t) = 1 - \prod_{i=1}^{q} (1 - R_i(t,\gamma)), \tag{30}$$

The reliability of complex systems is computed from a combination of the elementary functions (29) and (30).

Lemma 2. *In degraded functional conditions, the overall system reliability can be characterized by a baseline failure rate and the loss of effectiveness factors which give an image of the mean operating time of the reconfigured system.*

3.3. Reconfigurability with respect to reliability requirements. For reliable fault-tolerant control design, the admissible required energy corresponding to the acceptable degraded modes (18) is defined based on reliability evaluation. The reconfigurable reliable system achieves the control objective until the end of the mission with a high probability.

Definition 6. The system is *fault tolerant and reliable* with respect to the fault occurring at time $t = t_f$ for the control objective x_0 if the accommodation or the reconfiguration problem has an admissible solution with respect to the reliability requirement.

Lemma 3. *For the exponential distribution, the reliability constraint $R(t) \geq R_{\rm pth}$ is satisfied for every t during the mission, if the constraint is satisfied* a priori *at the end of the mission $t = t_m$.*

In order to compute the value of the admissible energy required under degraded functional conditions $\sigma_{\rm pth}$, we define the set of the acceptable degraded functional modes as follows:

$$\gamma^* = \{\gamma \in \mathbb{R}^m,\ \ R(t_m,\gamma) \geq R_{\rm pth}\}, \tag{31}$$

where γ^* is the set of effectiveness factors corresponding to degraded functional conditions which respect the reliability requirements. Based on (31) and (18), reliable fault-tolerant control design is available for an admissible solution defined by the required energy of the worst acceptable degraded case $\sigma_{\rm pth}$, corresponding to the maximum energy required for γ^*.

Definition 7. In degraded functional conditions, the solution of a reliable fault-tolerant control problem is *admissible with respect to a control objective* if

$$\rho(\gamma) \leq \rho_{\rm pth}, \tag{32}$$

where

$$\rho_{\rm pth} = \frac{\sigma_{\rm pth} - \sigma_{\min}}{\sigma_{\max} - \sigma_{\min}} \tag{33}$$

and

$$\sigma_{\rm pth} = \max(\sigma(\gamma^*)). \tag{34}$$

In fact, the indicator (33) is a reconfigurability index for reliable fault-tolerant control design, found based on energy with respect to reliability requirements.

4. Aircraft simulation example

To illustrate the different steps of the proposed approach, the model of an aircraft simulation used by Wu *et al.* (2000) is proposed. The plant model has two inputs (elevon command and canard command) and two outputs (angle of attack, pitch rate and pitch angle). This example is considered with two actuators in order to simplify the illustration of results. The values of the nominal failure rates associated to the actuators are presented in Table 1.

Table 1. Failure rates of elementary components.

Baseline failure rates	
λ_1^0	$9 \cdot 10^{-6}\ \mathrm{h}^{-1}$
λ_2^0	$5 \cdot 10^{-6}\ \mathrm{h}^{-1}$

The control objectives were originally specified on vertical transition, pitch pointing and direct lift. Around an operating point, the state-space description of the plant model is given by (1) with

$$A = \begin{bmatrix} -0.0226 & -36.6 & -18.9 & -32.1 \\ 0 & -1.9 & 0.983 & 0 \\ 0.0123 & -11.7 & -2.63 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

$$B = \begin{bmatrix} 0 & 0 \\ -0.414 & 0 \\ -77.8 & 22.4 \\ 0 & 0 \end{bmatrix},$$

$$C = \begin{bmatrix} 0 & 5.73 & 0 & 0 \\ 0 & 0 & 0 & 5.73 \end{bmatrix}.$$

The factors γ_1 and γ_2 of the actuator loss of effectiveness are introduced for each column of B by (2). The elevons are regarded as the primary control effectors, and the canards as the secondary, which could also produce secondary effects to the vehicle's lateral and directional motion when used differentially. First, the controllability Gramian is calculated by using the Lyapunov equation (12) for each degraded state, which is defined according to the different values of (γ_1, γ_2) with $0 \leq \gamma_i < 1$. In order to study the control reconfigurability of the plant, the index based on the normalization of energy consumption is calculated from (17). After reliability evaluation, this index is compared with the energy threshold ρ_{pth} found according to (33), which defines the worst acceptable degraded performance. Indeed, for this application, the overall system reliability is evaluated for each degraded functional mode according to (30). The failures rate are obtained according to (27).

The predefined reliability threshold $R_{\mathrm{pth}} = 95\%$ is fixed for this application. This value means that, after fault occurrence and for all reconfigurable degraded states, the probability that the system accomplishes the control objective until the end of the mission t_m should be higher than 0.95. The mission duration is considered for $t_m = 600$ min.

Figure 1 shows the evaluation of the overall system reliability $Rg(t_m)$ under degraded conditions, where the x and y axes represent respectively the studied actuators loss of effectiveness (γ_1, γ_2). In fact, the overall system reliability in each degraded mode (defined according to (γ_1, γ_2)) is compared with the reliability threshold R_{pth} which should be fulfilled after reconfiguration.

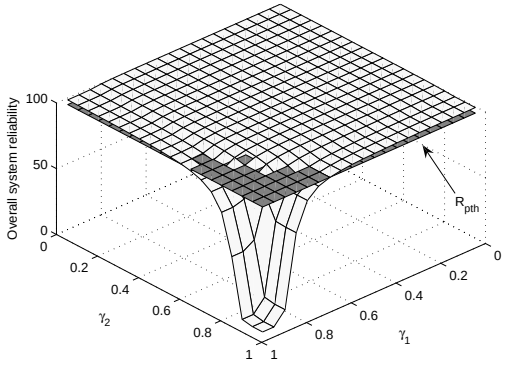


Fig. 1. Reliability evaluation at the end of the mission.

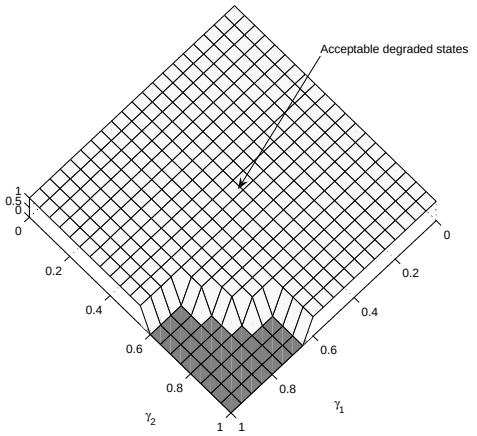


Fig. 2. Acceptable degraded states based on reliability evaluation.

The comparison of the overall system reliability and R_{pth} is shown in Fig. 2 where the result defines the set of the acceptable degraded states γ^*. Unity is assigned to the degraded modes that satisfy the reliability requirements and are considered as able to be tolerated if the required energy is admissible (31).

According to (34), the admissible required energy σ_{pth} which defines the maximum acceptable cost for reli-

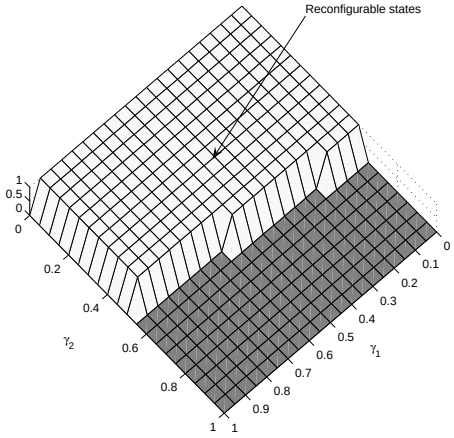


Fig. 3. Control reconfigurability based on energy with respect to reliability requirements.

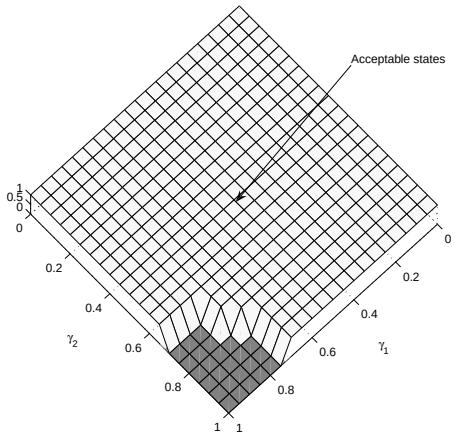


Fig. 4. Acceptable degraded states based on reliability evaluation.

able fault-tolerant control design can be found. By normalization, the reconfigurability index (33) and the energetic threshold $\rho_{\rm pth}$ are obtained. The acceptable degraded modes can be found according to (32). In fact, Fig. 3 shows the reconfigurable modes found according to admissibility solution (32) and the evaluation of the proposed reconfigurability index. Unity is assigned to the set of the reconfigurable states under degraded functional conditions defined according to the actuator loss of effectiveness (γ_1, γ_2).

These results show the advantage of integrating reliability analysis for reliable fault-tolerant control design. In fact, as can be shown, the maximum energy required to both tolerate actuator faults and achieve the control objective until the end of the mission with a high probability can established by using reliability analysis. For reliable fault-tolerant control design, the reconfigurable modes considered, which comply with the obtained energy threshold, minimize the energy consumption under degraded functional conditions and maintain the control objective until the predefined final time of the mission. All these admissible states minimize energy consumption and guarantee that the overall system reliability is above $R_{\rm pth}$.

However, since reliability is a probability measure in time, we evaluate the ability of reliable fault-tolerant control system design for different mission durations. The impact of time on actuator degradation can be shown for $t_m = 300$ min in Fig. 4. The acceptable degraded modes (31) which respect the reliability requirements are wider than in the previous scenario. Unity is assigned to the set γ^*. In fact, for a small mission period, the actuator degrades less rapidly and the set of the acceptable degraded modes is more extensive. By evaluation of the reconfigurability index (17) compared with (33), the corresponding reconfigurable modes are shown in Fig. 5. For this scenario, the proposed reliable fault-tolerant control design is able to tolerate more severe faults under more severe degraded conditions compared with the first scenario.

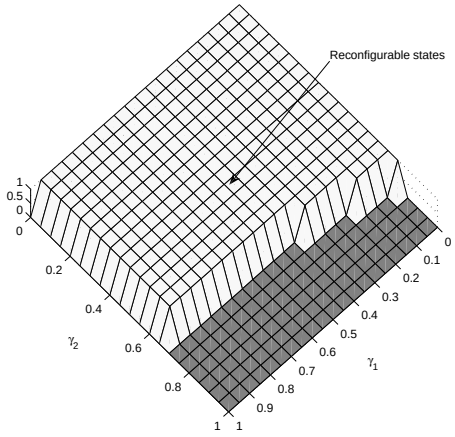


Fig. 5. Control reconfigurability for $t_m = 300$ min.

5. Conclusion

A reconfigurability index based on energy consumption with respect to reliability requirements has been proposed in this paper. The results obtained in this study prove that the solution for the admissibility of reliable design can be established by using overall system reliability evaluation, in addition to the energy criterion. Indeed, an admissible solution for control reconfigurability based on reliability analysis is proposed. This relation characterizes those states that are reachable (by acceptable degraded func-

tional conditions) in terms of energy consumption. For the proposed approach, on-line reliability computation of the system is not necessary. However, for an admissible solution characterized by the proposed reconfigurability index, the decision on reconfiguration can be made on-line.

In fact, the obtained results represent the data base of reconfigurable degraded functional modes for reliable fault-tolerant control design which can be checked and verified on-line. Moreover, it would be interesting as a future work to study system reconfigurability by evaluating the overall system reliability analytically. The aim is to guarantee the control objectives after a fault occurrence by energy minimization until the end of the mission with a high probability.

References

Blanke, M., Kinnaert, M., Lunze, J. and Staroswiecki, M. (2006). *Diagnosis and Fault Tolerant Control*, Control Systems, Vol. 2, Springer-Verlag, London.

Blanke, M., Staroswiecki, M. and Wu, E. (2001). Concepts and method in fault-tolerant control, *Proceedings of the American Control Conference, ACC 2001 Arlington, VA, USA*, Vol. 4, pp. 2606–2620.

Cox, D. (1972). Regression models and life tables, *Journal of the Royal Statistical Society* **34**(2): 187–220.

Frei, C., Karus, F. and Blanke, M. (1999). Recoverability viewed as a system property, *Proceedings of the European Control Conference, IEEE ECC'99, Budapest, Hungary*.

Gertsbakh, I. (2000). *Reliability Theory with Applications to Preventive Maintenance*, Springer-Verlag, Berlin/Heidelberg.

Gonzalez-Contreras, B., Theilliol, D. and Sauter, D. (2009). On-line reconfigurability evaluation for actuator faults using input/output data, *7th IFAC Symposium on Fault Detection, Supervision and Safety of Technical Processes, Barcelona, Spain*, pp. 674–679.

Guenab, F., Theilliol, D., Weber, P., Zhang, Y. and Sauter, D. (2006). Fault tolerant control design: A reconfiguration strategy based on reliability analysis under dynamic behavior constraints, *Prococeedings of the 6th IFAC SAFEPROCESS'06, Beijing, China*, pp. 1387–1392.

Khelassi, A., Theilliol, D. and Weber, P. (2009). Reconfigurability for reliable fault-tolerant control design, *7th Workshop on Advanced Control and Diagnosis, ACD'09, Zielona Góra, Poland*.

Khelassi, A., Weber, P. and Theilliol, D. (2010). Reconfigurable control design for over-actuated systems based on reliability indicators, *Proceedings of the Conference on Control and Fault-Tolerant Systems, IEEE SysTol 2010, Nice, France*, pp. 365–370.

Li, H., Zhao, Q. and Yang, Z. (2007). Reliability modeling of fault tolerant control systems, *International Journal of Applied Mathematics and Computer Science* **17**(4): 491–504, DOI: 10.2478/v10006-007-0041-0.

Martorell, S., Sanchez, A. and Serradell, V. (2009). Age-dependent reliability model considering effects of maintenance and working conditions, *Reliability Engineering and System Safety* **64**(1): 19–31.

Marusak, P.M. and Tatjewski, P. (2008). Actuator fault tolerance in control systems with predictive constrained set-point optimizers, *International Journal of Applied Mathematics and Computer Science* **18**(4): 539–551, DOI: 10.2478/v10006-008-0047-2.

Moore, B. (1981). Principal component analysis in linear systems: controllability observability and momdel reduction, *IEEE Transactions on Automatic Control* **26**(1): 17–32.

Noura, H., Theilliol, D., Ponsart, J. and Chamssedine, A. (2009). *Fault Tolerant Control Systems: Design and Practical Application*, Springer, Dordrecht/Heidelberg/London.

Patton, R. (1997). Fault-tolerant control: The 1997 situation, *Proceedings of IFAC SAFEPROCESS'97, Hull, UK*, pp. 1033–1055.

Staroswiecki, M. (2002). On reconfigurability with respect to actuator failures, *Proceedings of the 15th IFAC World Congress, IFAC 2002, Barcelona, Spain*, pp. 775–780.

Staroswiecki, M. (2003). Actuator faults and the linear quadratic control problem, *Proceedings of the 42nd Conference on Decision and Control, IEEE CDC'03, Maui, HI, USA*, pp. 959–965.

Tharrault, Y., Mourot, G., Ragot, J. and Maquin, D. (2008). Fault detection and isolation with robust principal component analysis, *International Journal of Applied Mathematics and Computer Science* **18**(4): 429–442, DOI: 10.2478/v10006-008-0038-3.

Wu, N., Zhou, K. and Salmon, G. (2000). Control reconfigurability of linear time-invariant systems, *Automatica* **36**(11): 1767–1771.

Yang, Z. (2006). Reconfigurabillity analysis for a class of linear hybrid systems, *Proceedings of 6th IFAC SAFEPROCESS'06, Beijing, China*, pp. 974–979.

Zhang, Y. and Jiang, J. (2008). Bibliographical review on reconfigurable tolerant-control system, *Annual Reviews in Control* **32**(2): 229–252.

Ahmed Khelassi received his M.Sc. degree in automatic engineering from the University of Bordeaux 1, France, in 2008. He is a Ph.D. student in the Research Centre for Automatic Control of Nancy (CRAN) at Nancy University, associated with the National Research Center for Science CNRS (UMR 7039). His research interests include fault-tolerant control, diagnosis, safety, reliability and aerospace systems.

Didier Theilliol received the Ph.D. degree in control engineering from Nancy University (France) in 1993. Since 2004, he has been a full professor in the Research Centre for Automatic Control of Nancy (CRAN) at Nancy University, where he co-ordinates and leads national, European and international R&D projects in steel industries, wastewater treatment plants, or aerospace domains. His current research interests include model-based fault diagnosis method synthesis and reliable active fault-tolerant control system design for LTI, LPV, multi-linear systems. Prof. Theilliol has published over 70 journal and conference papers.

Philippe Weber received the M.Sc. degree in automatic control and signal processing in 1995 from Henri Poincar Nancy University, France, and the Ph.D. degree in 1999 from the National Polytechnic Institute of Grenoble, France. He has been an assistant professor at Nancy University since 2000, and a member of the Research Centre for Automatic Control (CRAN) associated with the National Research Center for Science CNRS (UMR 7039). He focuses his interest on modeling problems in maintenance, prognosis and dynamic reliability. He develops fault-tolerant control systems including reliability analysis. Since 2000 his research interest has been focused on modeling methods based on Bayesian networks.

Received: 8 March 2010
Revised: 6 November 2010
Re-revised: 27 December 2010

Available online at www.sciencedirect.com
SCIENCE DIRECT
Reliability Engineering and System Safety 91 (2006) 149–162
RELIABILITY ENGINEERING & SYSTEM SAFETY
www.elsevier.com/locate/ress

Complex system reliability modelling with Dynamic Object Oriented Bayesian Networks (DOOBN)☆

Philippe Weber[a,*], Lionel Jouffe[b]

[a]Centre de Recherche en Automatique de Nancy (CRAN), UMR 7039 CNRS-UHP-INPL 2, rue Jean Lamour, 54519 Vandoeuvre-Les-Nancy Cedex, France
[b]Bayesia, 6, rue Léornard de Vinci, BP 0119, 53001 Laval, France

Received 15 October 2003; accepted 2 March 2005
Available online 24 May 2005

Abstract

Nowadays, the complex manufacturing processes have to be dynamically modelled and controlled to optimise the diagnosis and the maintenance policies. This article presents a methodology that will help developing Dynamic Object Oriented Bayesian Networks (DOOBNs) to formalise such complex dynamic models. The goal is to have a general reliability evaluation of a manufacturing process, from its implementation to its operating phase. The added value of this formalisation methodology consists in using the a priori knowledge of both the system's functioning and malfunctioning. Networks are built on principles of adaptability and integrate uncertainties on the relationships between causes and effects. Thus, the purpose is to evaluate, in terms of reliability, the impact of several decisions on the maintenance of the system. This methodology has been tested, in an industrial context, to model the reliability of a water (immersion) heater system.

Keywords: Dynamic Object Oriented Bayesian Networks (DOOBNs); Markov Chain; Reliability estimation

1. Introduction

One of the main challenges of the Extended Enterprise is to maintain and to optimise the quality of the services delivered by industrial objects in a dynamic way along their life cycle. The purpose is to conceive decision aiding systems to maintain the system in operation. Nevertheless, most of the automated systems do not provide the means of intelligent interpretation of the information when great process disturbances have to be considered. Moreover, decisions can be taken without a perfect perception of state of the system. This partial perception argues in favour of using a probabilistic estimation of the system state. As described in [9], tools issued from the Artificial Intelligence can be used to bring help in decision aiding systems of manufacturing processes.

Works on system safety and Bayesian Networks (BNs) were recently developed in [16] and the current works presented by Boudali and Dugan [5]. Bobbio et al. [6] explain how the Fault Tree (FT) can be implemented by using BNs. In the paper [7], the authors describe the stochastic modeling techniques as FT, BN and Petri Net. They present some application cases and highlight the advantages of each technique with respect to the others. Nevertheless, large and complex BNs are difficult to design and to maintain. This is the reason why the method proposed within the SERENE project [8] is interesting. This method is based both on BNs and on a hierarchical decomposition of the decision-making model for system safety analysis. Recent publications focus on Object Oriented Bayesian Networks (OOBNs) [3,4,18]. Indeed, they allow to implement the SERENE methodology based on Bayesian Networks.

The top down BNs construction that uses several levels of abstraction, and the powerful model elaboration mechanism for the models that have repetitive structures, make OOBNs very useful to model processes. Elementary models are then used and both the structure and the parameters can be improved through an analysis of past experiences.

Weber et al. [24], proposed a model-based decision system based on a static probabilistic model that allows to

☆ Revised version of the paper presented at QUALITA 2003.

* Corresponding author. Tel.: +33 (0)3 83 68 5127; fax: +33 (0)3 83 68 5012.
E-mail addresses: philippe.weber@esstin.uhp-nancy.fr (P. Weber), jouffe@bayesia.com (L. Jouffe).

0951-8320/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2005.03.006

diagnose faults by using an analysis of the system's functioning and malfunctioning. In order to improve diagnosis and maintenance strategies, our purpose is to define a dynamic model of the process behaviour. This model allows computing state probability distributions by taking into account both the age of the components and the latest maintenance operations.

The purpose of this paper is to introduce an Object Oriented Approach to model the system's reliability with Dynamic Bayesian Networks (DBNs) model. In [20], the authors demonstrate that DBNs are equivalent to Markov Chains (MCs). The problems that are considered here are those involving systems whose dynamics can be modelled as stochastic processes, in which the decision maker's actions influence the system's behaviour. The current state of the system and the action that is applied on that state determine the probability distribution over the next states. In the work [26], a study is dedicated to the comparison between MCs and DBNs for system reliability estimation, and the paper [27] describes the reliability modelling effectiveness of the DBNs to simulate a stochastic process with exogenous constraints.

This paper is divided into six sections. Section 2 presents the problem statement and highlights the main drawback of a model based on a MC model, i.e. the fast growing of the state space with respect to the system complexity. Section 3 describes the Bayesian Networks theory and defines the dynamic and the object oriented representation of BN used in the following. The proposed methodology is an original formalisation that can be useful to model system reliability (Section 4) by means of DOOBNs (Section 5). Finally, the simulation of a water heater system is developed in Section 6 and some conclusions and perspectives are discussed in Section 7.

2. Problem statement

In order to take, the uncertainty into account, the process state is considered as a random variable that takes its values in a finite state space corresponding to the set of all the possible process states. A MC allows to model the system dynamics over these states [9].

2.1. The Markov Chain notations in reliability

We will first of all define the notations used to describe the MC model. Let X be a discrete random variable used to model a process with a finite number of mutually exclusive states $\{s_1,\ldots,s_M\}$. The vector π, then, denotes a probability distribution over these states:

$$\pi = [\pi(s_1)\cdots\pi(s_m)\cdots\pi(s_M)],\ \pi(s_m)\geq 0$$
$$\text{with } \pi(s_m) = p(X = s_m) \text{ and } \sum_{m=1}^{M}\pi(s_m) = 1 \quad (1)$$

Assuming that the occurrence of events imply system state transitions, from a state at time step $(k-1)$ to a state at time step (k), the process produces a sequence $(\pi_0,\pi_1,\ldots,\pi_{k-1},\pi_k)$ that can be modelled as a discrete MC if: $\pi_k(s_m)=p(X_k=s_m|\pi_{k-1})$. The Markov property makes it possible to specify the statistical relationship among states as a transition probability matrix $\mathbf{P}_{MC}$. The MC is qualified as homogeneous if the state transition probabilities $p_{ij}=p(X_k=s_j|X_{k-1}=s_i)$ are time independent.

The reliability of a system can be modelled by using a MC. This method leads to a graphical representation ([1], p. 124). Let's consider the modelling of a component (entity). We will use a discrete random variable X with two states $\{up, down\}$ to represent, respectively, the operational and failure state of the component. The matrix $\mathbf{P}_{MC}$ described below defines the probabilistic state transitions between (*up*) and (*down*):

$$\mathbf{P}_{MC} = \begin{bmatrix} 1-p_{12} & p_{12} \\ 0 & 1 \end{bmatrix} \quad (2)$$

where p_{12} represents the failure probability of the component between time steps $(k-1)$ and (k); $p_{12}=p(X_k=down|X_{k-1}=up)$. Let T the time to failure of the component be a positive random variable with an exponential distribution $f(T)=\lambda\cdot e^{-\lambda\cdot t}$. In reliability studies, λ is the parameter known as the component failure rate. Then, we have: $p_{12}\approx\lambda\cdot\Delta t$ (see page 37 in [2]) where Δt represents the time interval between time steps $(k-1)$ and (k), λ being a probability per time unit (Fig. 1). In the following, Δt is assumed to be equal to 1 h. For constant failure rates, the Mean Time to Failure (MTTF) is defined (see page 87 in [10]): $\text{MTTF}=1/\lambda$.

2.2. Problem to model complex process

The MC method is suitable for computing the reliability of entity or system of low complexity. However, when we deal with complex systems with several components, we assist to a combinatorial explosion of the number of states that are necessary to model the system reliability, making MC unmanageable. To decrease the model's complexity, the hypothesis (a) according to which there is no simultaneous occurrence of failure is assumed. Even if this hypothesis simplifies the transition probability matrix, the number of states is still prohibitive for the modelling of complex real systems with MC.

In practice, to deal with this modelling problem, methods based on Fault Tree (FT) or Success Tree (ST) (p. 146 in [10]) can be used. These methods assume the statistical

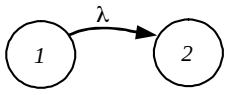


Fig. 1. Markov chain.

independence between events (hypothesis (b)), and they also assume that a static model of the situations is given. However, hypothesis (b) is no longer valid when components have common causes or when components have several failure modes.

Stochastic Petri Net ([19] and [11]) is also a method traditionally used to model the system reliability. Stochastic Petri Nets provide a powerful modelling formalism. Unfortunately, the reliability analysis relies on a Monte Carlo simulation procedure that requires a great number of simulations when very low probabilities are targeted.

The following part deals with a method that will allow to exploit the advantages of both the MC and the FT approaches within a single representation that does not assume the hypotheses (a, b) and that does not rely on a Monte Carlo simulation to calculate the systems reliability. This method is based on Dynamic Bayesian Networks.

3. Bayesian Network theory

BNs are probabilistic networks based on graph theory. Each node represents a variable and the arcs indicate direct probabilistic relations between the connected nodes. Variables are defined over several states. The DBNs allow to take into account time by defining different nodes to represent the variables at different time slices.

3.1. The Bayesian Network notations

BNs are directed acyclic graphs used to represent uncertain knowledge in Artificial Intelligence [15]. A BN is defined as a couple: $\mathcal{G}=((N,A),\mathcal{P})$, where (N,A) represents the graph; N is a set of nodes; A is a set of arcs; $\mathcal{P}$ represents the set of probability distributions that are associated to each node. When a node is not a root node, i.e. when it has some parent nodes, the distribution is a conditional probability distribution that quantifies the probabilistic dependency between that node and its parents.

A discrete random variable X is represented by a node $n\in N$ with a finite number of mutually exclusive states. States are defined on $\mathcal{S}_n:\{s_1^n,\ldots,s_{\mathrm{M}}^n\}$. The vector π^n denotes a probability distribution over these states as Eq. (1), where $\pi^n(s_m^n)$ is the marginal probability of n being in state s_m^n. In the graph depicted in Fig. 2, nodes n_i and n_j are linked by an arc. If $(n_i,n_j)\in A$ and $(n_j,n_i)\notin A$ then n_i is considered as a parent of n_j. The set of the parents of node n_j is defined as $pa(n_j)=n_i$.

In this work, the set $\mathcal{P}$ is represented with Conditional Probability Tables (CPT). Then, each node has an associated CPT. For instance, in Fig. 2, the nodes n_i and n_j are defined over the sets $\mathcal{S}_{n_i}:\{s_1^{n_i},\ldots,s_{\mathrm{M}}^{n_i}\}$ and $\mathcal{S}_{n_j}:\{s_1^{n_j},\ldots,s_L^{n_j}\}$. The CPT of n_j is then defined by the conditional probabilities $p(n_j|n_i)$ over each n_j state knowing its parents states (n_i). This CPT is defined as a matrix:

$$\mathbf{P}(n_j|pa(n_j)) = \begin{bmatrix} p(n_j=s_1^{n_j}|n_i=s_1^{n_i})\cdots p(n_j=s_L^{n_j}|n_i=s_1^{n_i}) \\ p(n_j=s_1^{n_j}|n_i=s_{\mathrm{M}}^{n_i})\cdots p(n_j=s_{\mathrm{L}}^{n_j}|n_i=s_{\mathrm{M}}^{n_i}) \end{bmatrix} \quad (3)$$

Concerning the root nodes, i.e. those without parent, the CPT contains only a row describing the a priori probability of each state.

Various inference algorithms can be used to compute marginal probabilities for each unobserved node given information on the states of a set of observed nodes. The most classical one relies on the use of a junction tree (see [15], p. 76). Inference in BN [13] then allows to take into account any state variable observation (an event) so as to update the probabilities of the other variables. Without any event observation, the computation is based on a priori probabilities. When observations are given, this knowledge is integrated into the network and all the probabilities are updated accordingly.

Knowledge is formalised as evidence. A *hard evidence* of the random variable X indicates that the state of the node $n\in N$ is one of the states $\mathcal{S}_n:\{s_1^n,\ldots,s_{\mathrm{M}}^n\}$. For instance X is in state s_1^n : $p(n=s_1^n)=1$ and $p(n=s_{m\neq 1}^n)=0$. Nevertheless, when this knowledge is uncertain, *soft evidences* can be used (see [22]). A soft evidence for a node n is defined as one that enables the updating of the prior probability values for the states of n. For example, X is in state s_1^n and s_{M}^n with the same probability and not in the other states: $p(n=s_1^n)=0.5$, $p(n=s_{\mathrm{M}}^n)=0.5$ and $p(n=s_{m\neq(1,\mathrm{M})}^n)=0$.

3.2. Dynamic Bayesian Network

A DBN is a BN that includes a temporal dimension. This new dimension is managed by time-indexed random variables X_i is represented at time step k by a node $n_{(i,k)}\in N$ with a finite number of states $\mathcal{S}_{n_i}:\{s_1^{n_i},\ldots,s_{\mathrm{M}}^{n_i}\}$. $\pi_k^{n_i}$ denotes the probability distribution over these states at time step k. Several time stages are represented by several sets of nodes $N_0,\ldots,N_k$. N_k includes all the random variables relative to time slice k ([14] and [9] p. 38–45).

An arc that links two variables belonging to different time slices represents a temporal probabilistic dependence between these variables. Then DBNs allow to model random variables and their impacts on the future distribution of other variables. Defining these impacts as *transition-probabilities* between the states of the variable at time step $k-1$ and those at time step k leads to the definition of CPTs, that are relative to inter-time slices, equivalent to the one defined in the previous section (Eq. (3)). With this model, the future slice (k) is conditionally independent of the past

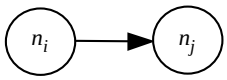


Fig. 2. A basic BN.

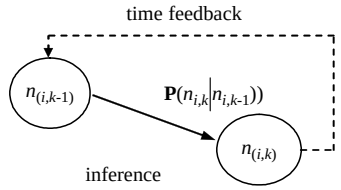


Fig. 3. A DBN for the random variable X_i.

given the present $(k-1)$, which means that the CPT $\mathbf{P}(n_{i,k}|pa(n_{i,k}))$ respects the Markov properties [17]. Moreover, this CPT is equivalent to the Markovian model of the variable X_i described in Section 2.1 if $pa(n_{i,k})=n_{i,k-1}$ and $\mathcal{S}_{n_{i,k-1}}=\mathcal{S}_{n_{i,k}}$ i.e.:

$$\mathbf{P}(n_{i,k}|n_{i,k-1})=\mathbf{P}_{\mathrm{MC}} \tag{4}$$

Starting from an observed situation at time step $k=0$, the probability distribution $\pi_k^{n_i}$ over n_i states is computed by the DBN inference. To compute $\pi_{k+T}^{n_i}$, several solutions are proposed in the literature. One of them consists in developing T time slices, resulting to a network size growing proportionally to T [17]. In this work, we have chosen another solution that allows keeping a compact network form, and that uses iterative inferences [28]. The notion of time is introduced through inference. Indeed, it is possible to compute the probability distribution of any variable X_i at time step k based only on the probabilities corresponding to time step $k-1$. The probability distributions at time step $k+1\ldots$ are computed using successive inferences. Then, a network with only two time slices is defined Fig. 3. The first slice contains the nodes corresponding to the current time step $(k-1)$, the second one those of the following time step (k). Observations, introduced as hard evidence or probability distributions, are only realised in the current time slice. The time increment is carried out by setting the computed marginal probabilities of the node at time step k as observations for its corresponding node in the previous time slice.

3.3. Object oriented Bayesian Networks

Modelling systems containing an important number of variables with BNs generally leads to complex models. To avoid this phenomenon, Koller has defined a particular class of BNs, the Object Oriented Bayesian Networks (OOBN) [18]. Their modelling is based on the decomposition of the global network into hierarchical levels [3,4]. This representation method allows to decentralize and to structure the knowledge within BNs of reduced size. Thanks to their structure, the OOBNs are then well suited for the modelling of industrial systems.

4. Reliability models with BN

Bayesian Networks provide a powerful mathematical formalism to model complex stochastic processes. The equivalence between Bayesian Networks and the classical Fault Trees method is described in the following section in the same way as it is in [6] and [5]. The comparison between Fault Trees and Bayesian Networks is done under the hypothesis of Fault Trees validity: in other words, events related to components or to functions can only be modelled with binary states. Then, the power of BN will be presented in the next section. We will argue that BNs are well suitable methods for the modelling of the complex propagation of failures through a probabilistic network of multimodal variables. This section will present the BN model of the dependent failure modes and the propagation of uncertainty. The last section will describe the dynamic BN and their equivalence to the Markov Chains.

4.1. Fault trees and Bayesian Networks to model reliability

A Fault Tree allows to describe the propagation logics of the failure across the system. System reliability or availability are modelled according to the assumption of independence between the events affecting the entities (hypothesis (a), see chapter 7 in [10]).

When components cannot be repaired, the basic fault events represent component failures. Under such conditions, the probability evaluation of fault trees based on the failure rates corresponds to the system reliability. The hypothesis (a) is then naturally respected. When components are repairable, the basic fault events depend on the failure and repair rate. Thus, the components' unavailability are computed using a Markov model and used as basic events in the FT. Under assumption (a), the probability evaluation of such fault trees corresponds to the system unavailability. Nevertheless, from a practical view point, hypothesis (a) is hardly verified. Indeed, in the case of a repairable system, the failure of a component generally has an effect on the behaviour of the other components. Therefore, in this paper the purpose is only to model the systems' reliability.

The following notation is adopted: (CMP=*up*) indicates that the component CMP is functioning, and (CMP=*down*) indicates that a failure has occurred (the component is then unable to perform its function). Fig. 4 and 5 compare elementary models of parallel components CMP1 and CMP2 that make up the system function S_3. Whereas a classical model of this parallel structure is based on a Fault Tree, the modelling with Bayesian Network is realized with

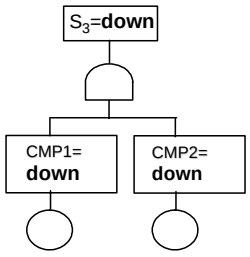
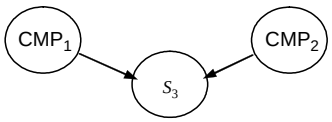


Fig. 4. Classical FT and ET models of parallel components.



$\mathbf{P}(S_3|CMP_1,CMP_2)$

	CMP_1	up		down	
	CMP_2	up	down	up	down
S_3	up	1	1	1	0
	down	0	0	0	1

Fig. 5. Equivalent BN of the parallel structure.

a single structure as depicted in Fig. 5 (the structure is identical for serial configurations). The CPT contains the conditional probabilities that translate the failure propagation logics across the functional architecture of the system. Therefore, the CPT is defined automatically by an OR/AND gate. These CPTs are a priori given, and probabilities are equal to 0 or 1 since the logic of the failure propagation is deterministic. To compute the reliability of the function S_3, events on component are considered as statistically independent ([12] and [23]):

$$\begin{aligned}
&\Pr(S_3 = up)_{\mathrm{ET}} = \Pr(\mathrm{CMP}_1 = up \cap \mathrm{CMP}_2 = up)\\
&\Pr(S_3 = down)_{\mathrm{FT}=}\Pr(\mathrm{CMP}_1 = down \cup \mathrm{CMP}_2 = down)\\
&\Rightarrow \Pr(S_3 = up)_{\mathrm{ET}} = \prod_{i=1}^{n} \mathbf{P}r(\mathrm{CMP}_i = up)\\
&\qquad = 1 - \prod_{i=1}^{2} \Pr(\mathrm{CMP}_i = down)\\
&\qquad = \Pr(S_3 = up)_{\mathrm{BN}}
\end{aligned} \tag{5}$$

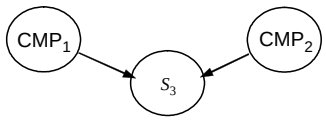
4.2. BN to model dependent failure modes and uncertain propagations

Thanks to the CPTs, BNs provide a model of the propagation of several failure modes in the system. Then, it is possible to synthetically represent in a factorised form system made up of entities with several failure modes. The hypothesis of independence between events (failures) made for FT is not necessary. Indeed, BNs allow computing exact repercussions of dependent variables to the system reliability. Moreover, it is possible to introduce uncertainty by setting probabilities in the interval of value [0, 1].

Failure Mode, Effects Analysis (FMEA) [23] allows to determine the failure modes associated with a component (Table 1). Therefore, the states (considered as exhaustive) of a CMP node are, for instance:

Table 1
FMEA

Failure modes	Causes	Effect
Function in mode 1	CMP failure1	Effect 1
	CMP failure2	Effect 2



$\mathbf{P}(S_3|CMP_1,CMP_2)$

	CMP_1	up		down1		down2	
	CMP_2	up	down	up	down	up	down
S_3	up	1	1	1	0	0.2	0
	down	0	0	0	1	0.8	1

Fig. 6. BN to model complex structure.

- *up:* the component is available,
- *down1:* the component is unavailable due to the failure 1,
- *down2:* the component is unavailable due to the failure 2 etc.

The states of function S_3 are defined by failure modes. For instance, node S_3 in the BN (Fig. 6) takes the following states: *up* or *down*. No prior probability is associated with these states because they are computed according to the states of their parents, i.e. the causes described by CMP_i nodes.

The CPT of the function S_3 is defined by using the columns of the causes and the failure modes of the FMEA analysis. Nevertheless, a BN representation can turn out to be useful insofar as a combination of causes (for instance $\mathrm{CMP}_1 = down2$ and $\mathrm{CMP}_2 = up$) can lead to several failure modes of the function with different probabilities. In Fig. 6, the uncertainty is represented by the probability distribution (0.2; 0.8).

As it is known in the FMEA analysis, a failure mode can happen to cause other failure modes according to the logics of the failure propagation through the system. The BN representation is able to model this propagation; nevertheless the construction of this model has to be structured. Section 5 of this paper presents a method to model the reliability of complex systems.

4.3. Dynamic Bayesian Networks to model entities

The reliability of low complexity components can be modelled as a DBN made up of two nodes as presented in Fig. 7. An MC model of component X_i reliability is easily translated into a DBN model [26]. Thus, independent components (entities) of the process are modelled using

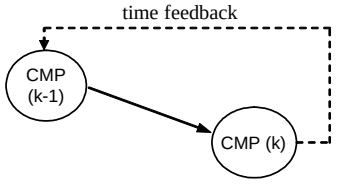


Fig. 7. Generic component DBN.

DBN equivalent to an independent MC. For instance, as it is defined in Section 2.1, a component is modelled by a discrete random variable X with states {*up*, *down*}. Then two nodes are defined to model the random variable at time slices (k) and ($k-1$): CMP(k) and CMP(k-1). These nodes, linked by an arc that represents the dependency between the component states at time step k and its states at time step ($k-1$), are both described by the states {*up*, *down*}.

Eqs. (2) and (4) define the CPT $\mathbf{P}(\mathrm{CMP}(k)|\mathrm{CMP}(k-1))$ linking the two time slices. The parameters are those defined to build the MC model of the component. To compute the probability $p(\mathrm{CMP}(k)=up)$ according to which the variable X_i is in the state *up* at (k), the following equation may be used:

$$p(\mathrm{CMP}(k) = up) = (1 - \lambda\Delta t)p(\mathrm{CMP}(k-1) = up) \qquad (6)$$

Eq. (6) corresponds to the classical formula of the discrete model of the MC.

5. Modelling approach

The main interest of such a method enabling a reliability modelling thanks to BNs lies in the propagation of the component failure states through the functionality of the system. Nevertheless, modelling complex systems requires a methodology that will help specify the BN's structure and the states of its variables. Methods like Structured Analysis and Design Technique (SADT) and FMEA are traditionally used in practice; therefore, we will endeavour to formalise the BN from this knowledge representation [25].

5.1. Unification of system functioning and malfunctioning knowledge

The model is elaborated before the implementation of the system. By that time, the main technological choices are made. But it is still necessary to define the logistics of maintenance, which contribute to reach goals in terms of performance. We propose here to design the BN model by using both the functional analysis (SADT) and the malfunctioning analysis of the system (FMEA). The definition of the environment, external resources, and failure modes are formalised at the level of the main function and Elementary Function (EF). The description of the components failures and reliability are made at the level of component (CMP).

The modelling approach consists, from the analysis of the systemic functioning based on SADT graphical representation [21], in representing the abnormal operation (malfunctioning) based on FMEA and then in formalising and unifying these two results in a unique model by means of OOBNs.

The functioning and malfunctioning of the system are dual and must be studied together to control each system variable. It leads, first, to focus on the system functioning in relation to its environment and its internal and external resources. This action can be made by using SADT graphical representation. This modelling is based on a principle of functional decomposition of the components, from functions and sub-functions to elementary functions.

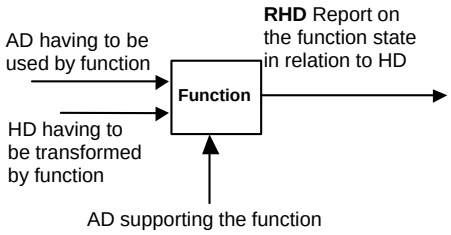


Fig. 8. Flows and function representation.

Each function (Fig. 8) represents a modification of a 'product' carried out by the system. It produces or consumes flows such as 'Having to Do' (HD) materialising the Input/Output (I/O) finality and 'being Able to Do' (AD) representing I/O energies, resources, activity support. From this step, simplifying assumptions are made for estimating the reliability. Therefore, the output flow is a report (RHD) that represents the function's finality. This flow is assumed to be the added value on the product flow represented in Fig. 8 by the Input HD flow that is transformed by the function. This output flow represents the functioning or failure modes of the function (as reliability of the function). Only the RHD flow is taken considered as output. It is thus transferred as informational view of physical result through the input flow of another function.

From this functioning, the malfunctioning is induced by considering that the relationship between these two modes is directly linked to the relationship between the normal and abnormal states of the variables. An FMEA analysis enables to create a malfunctioning model that helps identify the failure or degradation modes of each function, the elements that are responsible for the failure (causes) and the possible consequences of these failures (effects).

For example, the RHD flow can take the value *up* corresponding to the nominal state of the activity or the values *down1*, *down2* to identify the causes and the effects associated with these two abnormal states. The failure causes are either external (linked to the Input flows) or internal when they are linked to the AD function support flow (components). A set of states can thus be associated with each component. These states correspond to: nominal operation, failure 1, failure 2 etc.

In the same way, the consequences are observable either on function output flows or on the influence of the component degradation development on itself (to go towards a breakdown state). To sum up, a failure cause leads to a failure mode (e.g. the modification of the function state reported in RHD), which leads the function to be unable to produce the HD nominal flow any more.

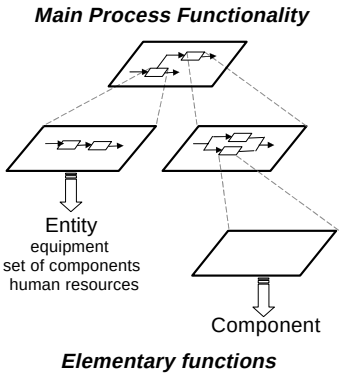


Fig. 9. Functional decomposition.

5.2. Reliability modelling with OOBN

The Bayesian Network representation is based on the functional decomposition of the system. The flows are represented by discrete random variables that are represented by the nodes of the BN. This representation is structured as a tree (Fig. 9). Its root is an OOBN representing the highest abstraction level. The elementary functions represent the lowest functional levels modelled by BNs. The connections between the sub-functions are modelled by logical functions. OOBNs are consist of generic sub-functions in the high functional levels of the model.

Then, a unified representation can be obtained by directly building OOBNs from the dual functioning/malfunctioning analysis presented above. To keep the concept of the generic function, inputs are modelled by input nodes defining the random variables associated with the flows AD, HD. The generic function represented in BN formalism is given in Fig. 10.

To model high functional levels, OOBNs are composed of generic sub-functions that are structured as in Fig. 10. When the function carries out several missions, it is possible to duplicate several inputs or outputs nodes (AD, HD…). Moreover, it is also possible to model sub-functions in parallel or in series (Fig. 11).

In Fig. 11, as the generic sub-functions F1 and F2 are in line, the report RHD1 is transferred to F2 through the input flow HD. As the functions F2 and F3 form a V structure, the node RHD is linked to RHD2 and RHD3 in order to compute the RHD of the overall function. The connections between

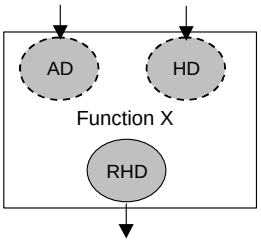


Fig. 10. Generic BN input and output nodes structure.

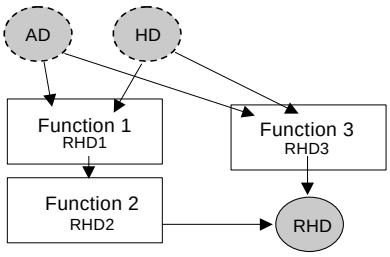


Fig. 11. High level of the functional decomposition.

functions are defined as CPT that represents the propagation logics of the failure modes, as it is presented Fig. 6.

OOBNs allow to describe systems thanks to serial or parallel component architectures. However, the CPTs—rather than the OOBN structures—constitute the relations of serial or parallel architectures.

Thus, the same relation between functions can be represented by the two different structures depicted in Figs. 12 and 13. This structural difference has no impact on the calculations of reliability if the CPT is defined as follows, where * is a logical operator representing the relation between functions F_1 and F_2:

- Fig. 12: the CPT of the node F3 defined $P(F_3|F_1,F_2) = P(F_1)*P(F_2)$.
- Fig. 13: the CPT models the transformation $P(X|F_1,F_2) = P(F_1)*P(F_2)$ and the CPT associated to F_3 ($P(X|F_3)$) corresponds to the identity operator (i.e. the CPT's diagonal is equal to 1, all the others probabilities being equal to 0).

These two structures are then equivalent. The choice of one structure rather than another depends on the specificity of the problem.

The OOBN model offers the possibility to compute the system reliability. However, equivalence between FTs and BNs is verified only if the system variables are described as binary. This restrictive hypothesis does not apply to BNs as they allow to consider random discrete variables defined on an unrestricted set of states. In short, a BN can always be defined as equivalent to a FT, but the reverse is false. Therefore, the modelling of failure modes by OOBN represents an increase of precision with respect to the reliability model.

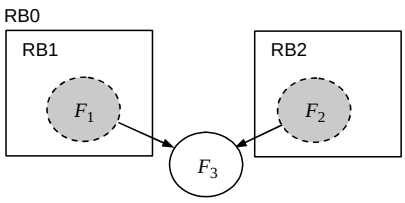


Fig. 12. RB: V structure

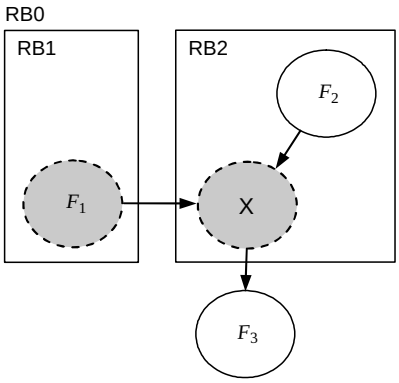


Fig. 13. RB: in line structure.

5.3. To model elementary function states related to components

If a component is used to perform several sub-functions, the output node CMP of the Component BN appears at the highest level containing the component. If a component performs only one sub-function (Elementary Function EF), the output node CMP appears as an AD flow supporting the function (Fig. 8) in a generic sub-function BN (Fig. 14).

The CMP output nodes are directly linked to the EF nodes representing their functionality. The CMP states are defined by the causes analysed by means of FMEA. The causes are either internal to the low BN level i.e. linked to CMP, or external, i.e. linked to the input nodes AD or HD. The common causes are defined in higher hierarchical levels and the information is forwarded by heritage between the levels through the input and output nodes.

The EF nodes are linked to the CMP nodes and to the input nodes leading to compute the RHD states probabilities (Fig. 14). If all the EFs are up then the RHD is up.

5.4. Model of components DOOBN

As for functions, a generic model is proposed for components (or for a set of components). Fig. 15 describes a Dynamic Object Oriented Bayesian Network (DOOBN) representing the model of a generic component: a component node CMP($k-1$) and its evolution defined as a Markov Chain modelled by the CPT of the node CMP(k).

It is now necessary to determine the probabilities associated with the states of the component. These probabilities depend on the reliability of the component.

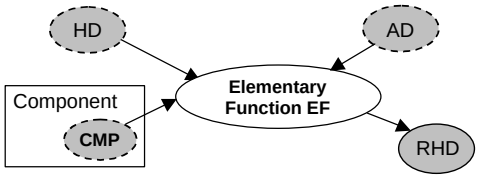


Fig. 14. Low level of the functional decomposition.

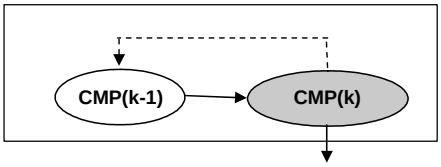


Fig. 15. Generic component BN.

Table 2
Component states and probabilities

CMP ($k=0$)	up (correct operation)	1
	down1 (cause of failure 1)	0
	down 2 (cause of failure 2)	0

Then, the probabilities associated with CMP(k) node states in the BN are estimated for a given operating time (Table 2).

The CMP(k) node is defined as an output node. Then, probabilities associated with the CMP(k) states are used to compute probabilities of the Elementary Function states related to this component.

5.5. Use of the model in operation: reliability estimator

The objective of the decision-making problems is to compare several alternative solutions (combination of decisions). The proposed model allows the simulation of several scenarios.

Once decisions have been taken, the BN model defined above can be used as an estimator of the system's reliability with respect to the chosen policy. The BN model allows to analyse the influences implied by the degradations on the functions' states. This analysis is based on the simulation of a component failure, a common cause or an unconformity of a sub-function. The objective is to forecast the impact of failures on the functions. It is then possible to analyse the upstream and downstream consequences on the whole system. For example, if we consider a component failure, an evidence can be set as $P(\text{CMP}=down1)=1$. The sub-functions probabilities are then updated by the BN inference. The RHD of each function relates the failure impact on each functional level.

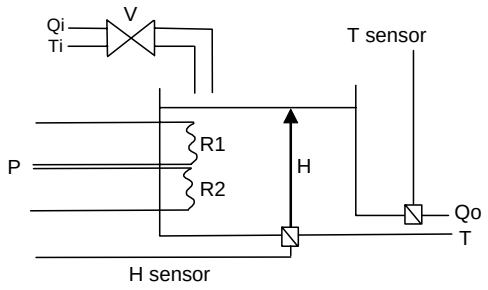


Fig. 16. Thermal process.

Table 3
FMEA-Component states

Function	Element	Failure mode	Effects	Causes
to transform pressure to Q_i	VALVE V	Remains closed	$Q_i=0$	No energy from (AD), Valve is down (state 4)
		Remains open	$Q_i>0$	No energy from (AD), valve is down (state 3)
		The water flow rate is biased	Q_i different from the desired Q_i	Valve is down (state 2)
to stock water Q_i to H	TANK	Leak of water	Water loss in the environment	Tank is down (state 2) Fissure
to transform H to Q_o	WATER PIPE	Clogged	$Q_o=0$	Pipe is down (state 3)
		Restricted	$Q_o<$ desired Q_o	Pipe is down (state 2)
to heat water from T_i to T	HEATING RESISTOR	Maximum level of heat	$T>$ desired T	Heating resistor is down (state 2)
		No heating	$T=T_i=20$ °C	No energy from (AD), Heating resistor is down (state 4)
		Heating power loss	$T<$ desired T	Heating resistor is down (state 3)
to measure H	H SENSOR	Biased measure	Q_o is different from the real Q_o	H sensor is down (state 2)
		No measure	Impossibility to control Q_o	No energy from (AD), H sensor is down (state 3)
to measure T	T SENSOR	Biased measure	T is different from the real T	T sensor is down (state 2)
		No measure	Impossibility to control P	No energy from (AD), T sensor is down (state 3)
to control V and P	COMPUTER	Control loss	Deviation of T and H	No energy from (AD), Computer is down (state 2)

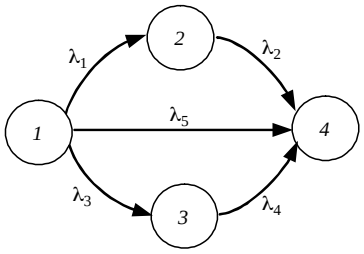
6. Application

The proposed method is applied to a classical example of a water heater process. The objective of the thermal process (show in Fig. 16) is to ensure a constant water flow rate with a given temperature. The process is composed of a tank equipped with two heating resistors $R1$ and $R2$.

The system inputs are the water flow rate Q_i, the water temperature T_i and the heater electric power P that is controlled by a computer. The outputs are the water flow rate Q_o and the temperature T that are regulated around an operating point ($Q_i=Q_o=20$ l min^{-1} and $T=50$ °C). The input temperature of the water $T_i=20$ °C is assumed to be constant.

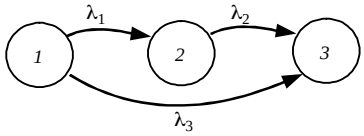
The components of this system are indexed in the FMEA analysis (Table 3). The failure modes of each component are defined as well as their effects. The causes are linked with the component states or the unavailability of the electric energy required to supply the component. Therefore, the loss of energy is a common cause of the six failure modes.

The figures (Figs. 17–23) present the Mean Time To Failure (MTTF) parameter allowing to determine the failure rates quantifying the transition between component states. These figures depict the Markov Chains of the components, which are considered, in this study, as independent. State 1 represents a component without failure.



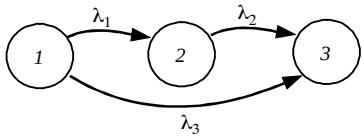
$MTTF_1$=10 000 h	$\lambda_1=1\ 10^{-4}$ h^{-1}
$MTTF_2$=500 h	$\lambda_2=20\ 10^{-4}$ h^{-1}
$MTTF_3$=7 000 h	$\lambda_3=1.43\ 10^{-4}$ h^{-1}
$MTTF_4$=2 000 h	$\lambda_4=5\ 10^{-4}$ h^{-1}
$MTTF_5$=15 000 h	$\lambda_5=0.66\ 10^{-4}$ h^{-1}

Fig. 17. HEATING RESISTOR reliability MC model.



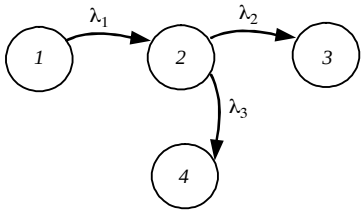
$MTTF_1$=5 000 h	$\lambda_1=2\ 10^{-4}$ h^{-1}
$MTTF_2$=3 000 h	$\lambda_2=3.3\ 10^{-4}$ h^{-1}
$MTTF_3$=45 000 h	$\lambda_3=0.22\ 10^{-4}$ h^{-1}

Fig. 18. H SENSOR reliability MC model.



$MTTF_1$=5 000 h	λ_1=2 10^{-4} h^{-1}
$MTTF_2$=3 000 h	λ_2=3.3 10^{-4} h^{-1}
$MTTF_3$=45 000 h	λ_3=0.22 10^{-4} h^{-1}

Fig. 19. T SENSOR reliability MC model.



$MTTF_1$=5 000 h	λ_1=2 10^{-4} h^{-1}
$MTTF_2$=3 000 h	λ_2=3.3 10^{-4} h^{-1}
$MTTF_3$=6 000 h	λ_3=1.66 10^{-4} h^{-1}

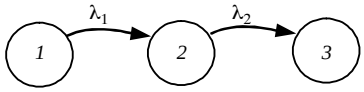
Fig. 20. VALVE V reliability MC model.

The process is made of seven components that have 2, 3 or 4 states. Modelling the system with a Markov Chain leads to define 1728 states ($4\times2\times3\times4\times3\times3\times2=1728$). The system's reliability is then computed according to the transition matrix $\mathbf{P}_{MC}$ that defines the probabilities linking all the states. This matrix requires approximately three million parameters.

Therefore, the reliability estimation of this process from the MC model is very difficult to obtain. In the following, the DOOBN modelling proves to be a more efficient and convenient tool. This model is a unified representation of the knowledge formalised from FMEA, SADT analysis, and independent MC of components.

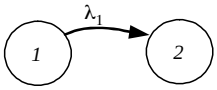
6.1. SADT analysis

Fig. 24 presents the level A0 of the system SADT analysis. This figure depicts the interaction between



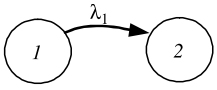
$MTTF_1$=5 000 h	λ_1=2 10^{-4} h^{-1}
$MTTF_2$=10 000 h	λ_2=1 10^{-4} h^{-1}

Fig. 21. WATER PIPE reliability MC model.



$MTTF_1$=40 000 h	λ_1=0.25 10^{-4} h^{-1}

Fig. 22. TANK reliability MC model.



$MTTF_1$=8 000 h	λ_1=1.25 10^{-4} h^{-1}

Fig. 23. COMPUTER reliability MC model.

the system and the external environment through the AD, HD and RHD flows. The main functionality of the process is:

- to provide warm water.

The next figure presents the level A0 describing the four functions that are necessary to perform the main task of the system (Fig. 25):

- to transform pressure into Q_i (A1),
- to control V and P (A2),
- to transform Q_i into H and T_i into T (A3),
- to transform H into Q_o.

Fig. 27 formalises the function 'to transform Q_i into H and T_i into T' from the elementary functions:

- to stock water supported by the component TANK,
- to heat water supported by the component HEATING RESISTOR.

6.2. DOOBN model

The DOOBN model is depicted in Figs. 26 and 29–31. The Dynamic Bayesian Network that models

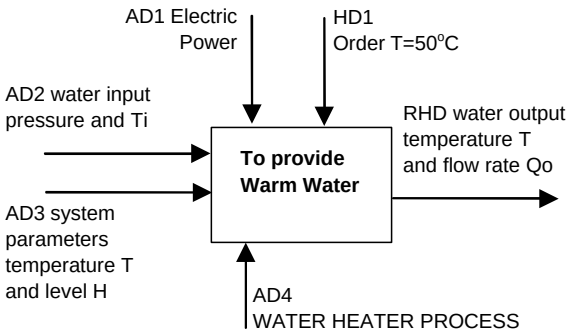


Fig. 24. SADT level A0.

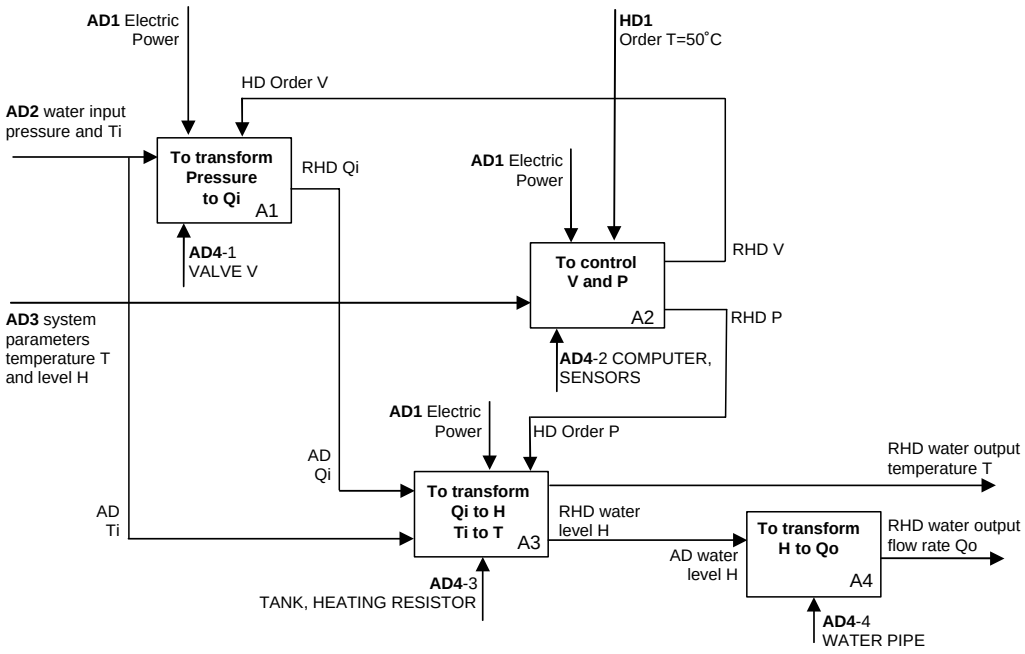


Fig. 25. SADT level A0.

the component HEATING RESISTOR, is presented in Fig. 26. The conditional Probability Table describes the independent Markov Chain that models the reliability of this component. Inferences are realised by using the BayesiaLab (β *version*) software (http://www.bayesia.com) that uses an iterative procedure to compute probabilities. The states probabilities are presented in the Fig. 28 according to the current time step (k). A maintenance action is simulated when $k=1000$ h. This maintenance action is assumed to be perfect, i.e. the component is reset in state 1 (no failure, no degradation). This event is simulated in order to illustrate its propagation through the model.

The propagation through the Object Oriented Bayesian Network model allows to take into account the dependency

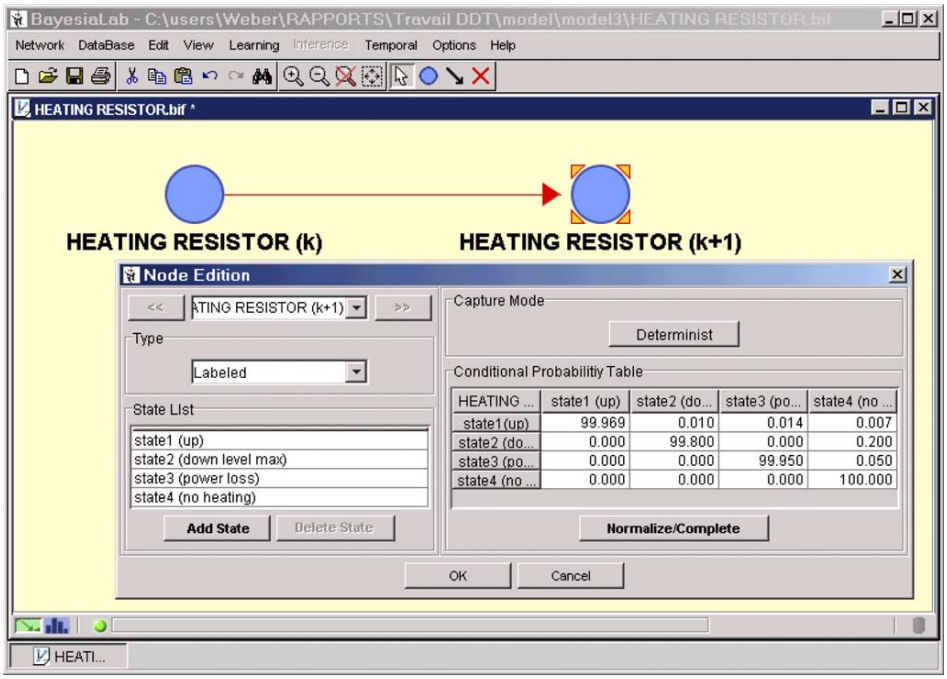


Fig. 26. Dynamic Bayesian Network model of the HEATING RESISTOR.

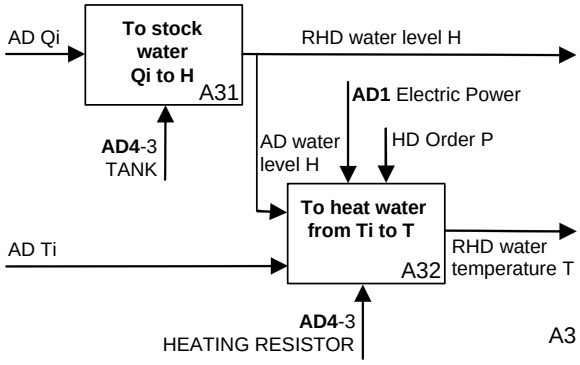


Fig. 27. SADT level A3 'to transform Q_i to H and Ti to T'.

between the failure modes and the common cause to compute the system's reliability $R(k)$. The Figs. 29–31 present OOBN models corresponding, respectively, to the SADT levels A3, A31 and A32 (see Fig. 27).

The elementary function 'EF to heat water' is supported by the component HEATING RESISTOR (Fig. 31), and depends on the states of the flows:

- AD electric power,
- AD T_i,
- AD water level H,
- HD order P.

This elementary function is described by four states according to the FMEA (Table 3). These states correspond to the following failure modes:

- State 1: function to heat water is correct.
- State 2: function to heat water is incorrect, the heating level is maximum.
- State 3: function to heat water is incorrect, the heating level is lower than the required level.
- State 4: function to heat water is incorrect, the heating level is equal to zero.

Probabilities related to these states are depicted in Fig. 32. The maintenance action with the component

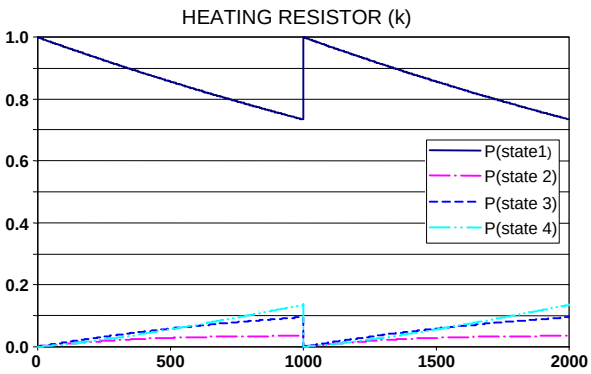


Fig. 28. States probabilities of the HEATING RESISTOR.

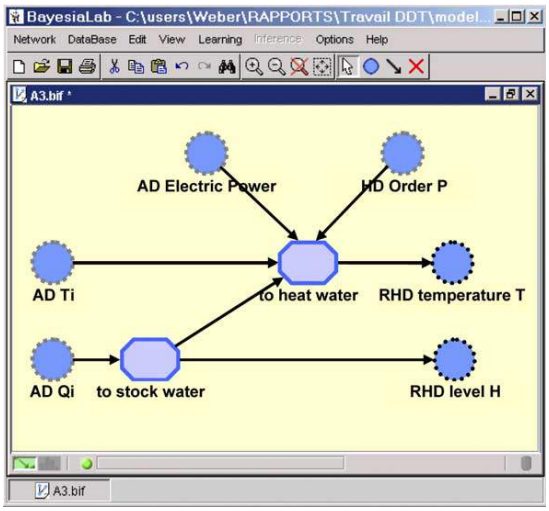


Fig. 29. OOBN model of A3 SADT level.

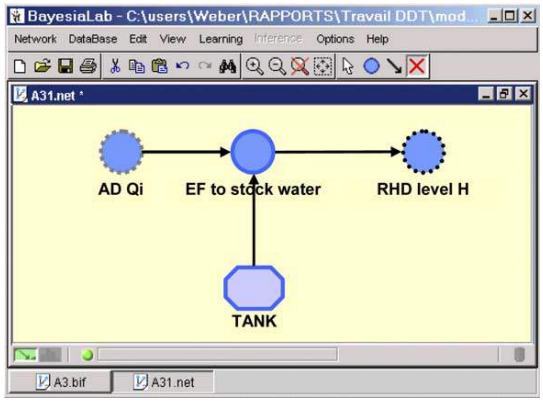


Fig. 30. OOBN model of A31 SADT level.

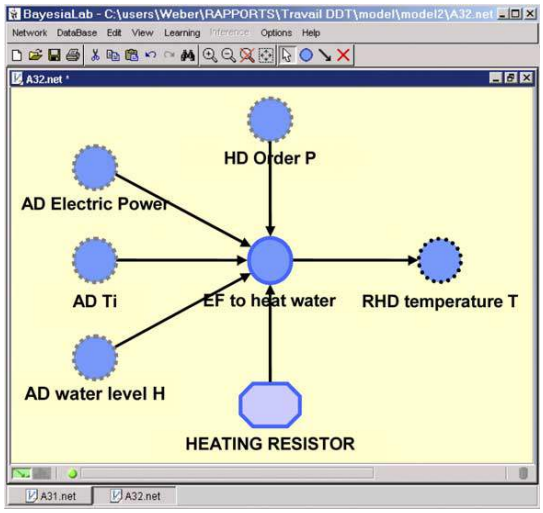


Fig. 31. OOBN model of A32 SADT level.

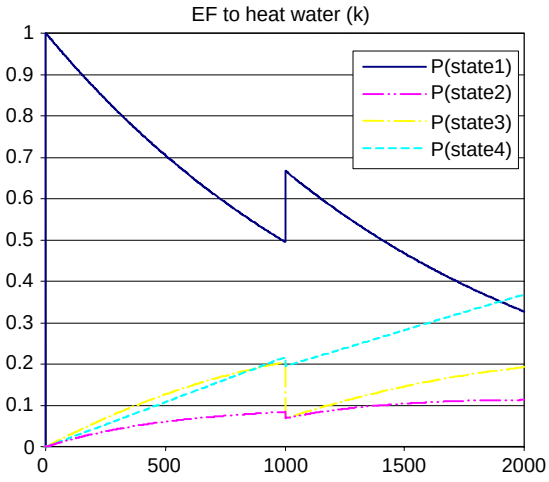


Fig. 32. States probabilities of the elementary function: to heat water.

HEATING RESISTOR has an impact on the 'EF to heat water' states. P(state1) increases and the other probabilities decrease. Nevertheless, in spite of the assumptions of a perfect maintenance action, P(state1) is less than 1. This is due to the failure and the degradation of the other components. The ageing of the system results in a degradation of the input flows (for example: AD level H or HD Order P) of the function 'to heat water'. Then, the 'EF to heat water' cannot be perfectly performed.

The objective of the system is to provide warm water at temperature T with flow rate Q_o. The reliability of the system depends on the states of the functions: to transform Q_i into H and T_i into T; to transform H into Q_o.

Fig. 33 presents the states of the flow 'RHD output water temperature T' and Fig. 34 presents the states of the flow 'RHD output water flow rate Q_o'. The 'RHD output water temperature T' is sensitive to the maintenance event. This is not the case for the flow 'RHD output water flow rate Q_o'

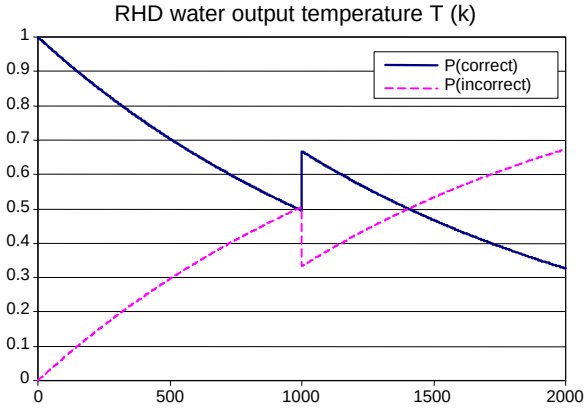


Fig. 33. States probabilities of the flow 'RHD water output temperature T'.

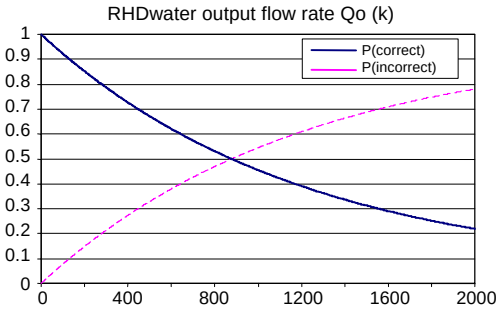


Fig. 34. States probabilities of the flow 'RHD water output flow rate Qo'.

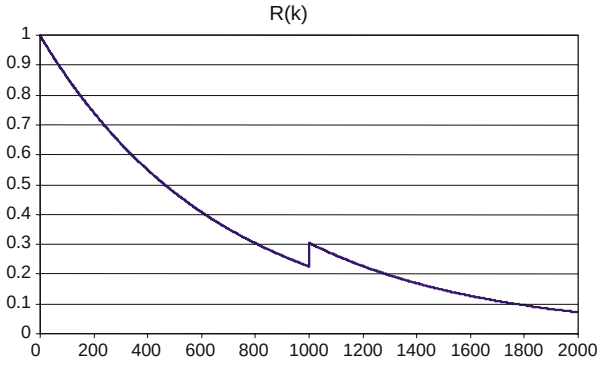


Fig. 35. Reliability of the system.

since the water level is assumed to be controlled independently from the water temperature.

Fig. 35 presents the reliability of the system and allows to observe the impact of the event corresponding to the maintenance of the HEATING RESISTOR.

7. Conclusion

The proposed method, based on the Dynamic Bayesian Networks and Object Oriented Bayesian Networks theory, easily allows designing DOOBN structures to model the temporal behaviour of the probabilities of complex system states. The correspondence between Markov Chain, Fault Tree Event Tree and DBN is presented and applied to the system reliability estimation.

Our method turns out to be a satisfying solution as far as the modelling of complex systems is concerned. Indeed, the number of states needed to model a complex system with MC increases exponentially (one state for each combination of elementary states). As the DBNs representation is based on the modelling of process entities, the obtained model is more compact and readable than the MC model. Furthermore, the dependency between several failure modes of a component and common modes is easily modelled by BN.

This paper shows that DOOBNs represent a very powerful tool for decision-making in maintenance.

In future works, in order to achieve this modelling technique, we have to define to what extent the learning algorithms of BN can contribute to model the dynamics of the system's reliability, and how the parameters' behaviour can then be modelled.

References

[1] Ansell JI, Phillips MJ. Practical methods for reliability data analysis. New York: Oxford University Press Inc; 1994. ISBN 0 19 853664 X.

[2] Aven T, Jensen U. Stochastic models in reliability. In: Karatzas I, Yor M, editors. Applications of mathematics: 41. New York: Springer; 1999. ISBN 0-387-98633-2, SPIN 10695247.

[3] Bangso O, Wuillemin P-H. Top-down construction and repetitive structures representation in Bayesian Networks. Thirteenth international Florida artificial intelligence research symposium conference, Florida, USA; 2000.

[4] Bangso O, Wuillemin P-H. Object Oriented Bayesian Networks. A framework for topdown specification of large Bayesian Networks and repetitive structures. AALBORG University Technical Report; September 2000.

[5] Boudali H, Dugan JB. A discrete-time Bayesian network reliability modeling and analysis framework. Reliab Eng Syst Safe 2005;87: 337–49.

[6] Bobbio A, Portinale L, Minichino M, Ciancamerla E. Improving the analysis of dependable systems by mapping fault trees into Bayesian Networks. Reliab Eng Syst Safe 2001;71(3):249–60.

[7] Bobbio A, Ciancamerla E, Franceschinis G, Gaeta R, Minichino M, Portinale L. Sequential application of heterogeneous models for the safetyanalysis of a control system: a case study. Reliab Eng Syst Safe 2003;81(3):269–80.

[8] Bouissou M, Martin F, Ourghanlian A. Assessment of a safety-critical system including software: a Bayesian belief Network for evidence sources. RAMS'99 reliability and maintainability symposium, Washington, USA; 1999.

[9] Boutillier C, Dean T, Hanks S. Decision-theoretic planning: structural assumptions and computational leverage. J Artif Intell Res 1999;11: 1–94.

[10] Dhillon BS. Design reliability: fundamentals and applications. New York: CRC Press LLC; 1999. ISBN 0-8493-1465-8.

[11] Dutuit Y, Châtelet E, Signoret J-P, Tomas P. Dependability modelling and evaluation by using stochastic Petri nets: application to two test cases. Reliab Eng Syst Safe 1997;55:117–24.

[12] Hoyland A, Rausand M. System reliability theory: models and statistical methods. New York: Wiley; 1994.

[13] Huang C, Dawiche A. Inference in belief networks: a procedural guide. Int J Approx Reason 1996;15:225–63.

[14] Hung KB, Venkatesk S, West G. Layered dynamic probabilistic networks for spatio-temporal modelling. Intell Data Anal 1999;3: 339–61.

[15] Jensen FV. An introduction to Bayesian Networks. London: UCL Press (Ed); 1996.

[16] Kang CW, Golay MW. A Bayesian belief network-based advisory system for operational availability focused diagnosis of complex nuclear power systems. Expert Syst Appl 1999;17:21–32.

[17] Kjaerulff U. dHugin: a computational system for dynamic time-sliced Bayesian Networks. Int J Forecasting 1995;11:89–111.

[18] Koller D, Pfeffer A. Object Oriented Bayesian Networks. In: Proceeding of the thirteenth annual conference on uncertainty in artificial intelligence (AI-97). Rhode Island, USA; July 1997.

[19] Nourelfath M, Dutuit Y. A combined approach to solve the redundancy optimization problem for multi-state systems under repair policies. Reliab Eng Syst Safe 2004;86:205–13.

[20] Padhraic S. Belief networks, hidden Markov models, and Markov random fields: a unifying view. Pattern Recognit Lett 1997;18: 1261–8.

[21] Santarek K, Buseif I. Modeling and design of flexible manufacturing systems using SADT and Petri nets tools. J Mater Process Technol 1998;76:212–7.

[22] Valtorta M, Kim YG, Vomlel J. Soft evidential update for probabilistic multiagent systems. Int J Approx Reason 2002;29: 71–106.

[23] Villemeur A. Reliability, availability, maintainability and safety assessment: methods and techniques. New York: Wiley; 1992 (Translated from French Edition, 1991 by Cartier A. and Lartisien MC; 1992).

[24] Weber P, Suhner MC, Iung B. System approach-based Bayesian Network to aid maintenance of manufacturing process. Sixth IFAC symposium on cost oriented automation, low cost automation, Berlin 2001.

[25] Weber P, Suhner MC. An application of Bayesian Networks to the performance analysis of a process. In: Proceedings of $\lambda\mu$ 13, ESREL 2002 European conference. Lyon, France; 2002.

[26] Weber P, Jouffe L. Reliability modelling with dynamic Bayesian Networks. 15th IFAC symposium on fault detection, supervision and safety of technical processes (SAFEPROCESS'03), Washington, DC, USA; 2003.

[27] Weber P, Munteanu P, Jouffe L. Dynamic Bayesian Networks modelling the dependability of systems with degradations and exogenous constraints. 11th IFAC symposium on information control problems in manufacturing (INCOM'04). Brazil: Salvador-Bahia; 2004.

[28] Welch R, Thelen T. Dynamic reliability analysis in an operational context: the Bayesian network perspective. In: Smidts C, Devooght J, Labeau PE, editors. Dynamic reliability: future directions. ISBN 0-9652669-3 1. Maryland, USA.